S. HRG. 116–122

EXPORT CONTROL REFORM IMPLEMENTATION: OUTSIDE PERSPECTIVES

HEARING

BEFORE THE

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

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

ON

CONDUCTING OVERSIGHT ON IMPLEMENTATION OF THE EXPORT CONTROL REFORM ACT (ECRA)

JULY 18, 2019

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

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

U.S. GOVERNMENT PUBLISHING OFFICE

39–542 PDF WASHINGTON : 2020

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

MIKE CRAPO, Idaho, *Chairman*

RICHARD C. SHELBY, Alabama	SHERROD BROWN, Ohio
PATRICK J. TOOMEY, Pennsylvania	JACK REED, Rhode Island
TIM SCOTT, South Carolina	ROBERT MENENDEZ, New Jersey
BEN SASSE, Nebraska	JON TESTER, Montana
TOM COTTON, Arkansas	MARK R. WARNER, Virginia
MIKE ROUNDS, South Dakota	ELIZABETH WARREN, Massachusetts
DAVID PERDUE, Georgia	BRIAN SCHATZ, Hawaii
THOM TILLIS, North Carolina	CHRIS VAN HOLLEN, Maryland
JOHN KENNEDY, Louisiana	CATHERINE CORTEZ MASTO, Nevada
MARTHA MCSALLY, Arizona	DOUG JONES, Alabama
JERRY MORAN, Kansas	TINA SMITH, Minnesota
KEVIN CRAMER, North Dakota	KYRSTEN SINEMA, Arizona

GREGG RICHARD, *Staff Director*

JOHN V. O'HARA, *Chief Counsel for National Security Policy*
JAMES GUILIANO, *Professional Staff Member*

LAURA SWANSON, *Democratic Deputy Staff Director*
COLIN MCGINNIS, *Democratic Policy Director*

CAMERON RICKER, *Chief Clerk*
SHELVIN SIMMONS, *IT Director*
CHARLES J. MOFFAT, *Hearing Clerk*
JIM CROWELL, *Editor*

C O N T E N T S

THURSDAY, JULY 18, 2019

	Page
Opening statement of Chairman Crapo	1
Prepared statement	21
Opening statements, comments, or prepared statements of:	
Senator Brown	3
Prepared statement	22
Senator Tester	4

WITNESSES

Eric L. Hirschhorn, Former Under Secretary for Industry and Security, Department of Commerce	5
Prepared statement	23
Responses to written questions of:	
Chairman Crapo	35
Senator Brown	39
Senator Warren	39
Senator Cortez Masto	40
Senator Sinema	43
Nova J. Daly, Former Deputy Assistant Secretary of Treasury for Investment Security (2006–2009) and Senior Public Policy Advisor, Wiley Rein LLP	7
Prepared statement	27
Responses to written questions of:	
Chairman Crapo	43
Senator Brown	47
Senator Warren	49
Senator Cortez Masto	51
Senator Sinema	52
Ben Buchanan, Ph.D., Assistant Teaching Professor, School of Foreign Service Senior Faculty Fellow, Center for Security and Emerging Technology, Georgetown University	9
Prepared statement	32
Responses to written questions of:	
Chairman Crapo	53
Senator Warren	54
Senator Sinema	55

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Letter submitted by Dennis Ralston, Sr. Director—Government Affairs and Cooperative R&D, KLA	56

EXPORT CONTROL REFORM IMPLEMENTATION: OUTSIDE PERSPECTIVES

THURSDAY, JULY 18, 2019

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

The Committee met at 10:04 a.m. in room SD–538, Dirksen Senate Office Building, Hon. Mike Crapo, Chairman of the Committee, presiding.

OPENING STATEMENT OF CHAIRMAN MIKE CRAPO

Chairman CRAPO. The hearing will come to order.

No one can dispute that technological advances are of vital importance to United States progress and development, where progress in knowledge and innovations undergird the growth of our U.S. productivity.

The U.S.-China Commission found that about half of the U.S. GDP and two-thirds of its productivity gains is attributable to U.S. technological improvements.

In August of 2018, the President signed the Foreign Investment Review Modernization Act, called "FIRRMA," and the Export Control Reform Act, known as "ECRA," into law.

FIRRMA is designed to strengthen the existing regulatory architecture in significant ways to deal with inbound foreign investments that would have the potential to threaten U.S. national security interests.

ECRA importantly reauthorizes an otherwise moribund Export Administration Act, continued only by annual reissuances of Presidential national security declarations.

It authorizes the Bureau of Industry and Security, or BIS, at Commerce to update controls on exports designed to prevent certain U.S. dual-use technologies, lower-level military items, and other things from ending up in the wrong hands.

These two important, hugely bipartisan bills were intended, in no small part, to ensure that with proper controls in place to establish highly guarded inward and outward regimes, a productive relationship between the United States and China is not only possible, but could be of the highest value in terms of global prosperity and security.

Today's hearing picks up where the Committee left off when it last looked at assessing investment controls on technology in its June 4th hearing on "Confronting Threats from China."

On June 4th, we examined China's intention to secure global technological leadership for itself, with a particular emphasis on

some of its inbound foreign direct investment strategies, particularly into the U.S. semiconductor industry.

Today the Committee shifts gears slightly to examine control issues surrounding exports of things outbound from the United States and other re-exports or transfers that may occur abroad.

Right now there is a raft of export control regulation on the horizon at the Commerce Department.

So far BIS is actively engaged on two rulemaking fronts covering "emerging and foundational technologies," which include technologies from such sectors as artificial intelligence, computing, additive manufacturing, data analytics, robotics, surveillance, and a long list of others.

Importantly, the items that BIS designates as "emerging technology" will also be deemed to be "critical technology" under FIRRMA and subject many potential inbound investment deals to CFIUS review notification requirements.

The current rulemaking under consideration at BIS is not set in stone.

It is busy poring over a myriad of industry and governmental comments that will inform its application of strict controls over emerging technologies, which industry will use to understand to whom it can transfer these technologies, who can otherwise use them, and who can even research them.

The Committee has before it a very accomplished panel of witnesses assembled to help us pull apart the underlying risks associated with the United States continuing its robust international economic relationships, including that with China, against preserving U.S. technological leadership over these emerging and foundational technologies and some of the more sensitive items that that would produce.

In the past, export controls sometimes have not been able to keep up with innovation, and this problem is exacerbated by today's pace of advancements, particularly in "artificial intelligence," which owing to its nature is itself a difficult sector to control.

Considering that BIS is very unlikely to designate all artificial intelligence technology, we are fortunate to have Dr. Buchanan here today to help the Committee better understand what "artificial intelligence" means, how it works, and why or why not certain aspects are more controllable than others.

Our professional export control experts, Mr. Hirschhorn and Mr. Daly, are expected to offer their assessments on how BIS may establish controls that address emerging and foundational technologies, while preserving the innovative capacity of the United States.

Before I turn to Senator Brown for his statement, let me indicate that I am going to have to step out for hopefully not too long to go to the Judiciary Committee where legislation dealing with AML BSA issues and other aspects that are of great interest and jurisdiction of this Committee are being considered at this moment. So I am going to have to step down there. I will turn it over to you, Senator Brown, and please take charge while I am gong.

Senator BROWN. [Presiding.] I will give my opening statement, then call on you, and I will start with Senator Toomey if Senator

Crapo is not back for questions if you are here. If you are not, then I will start.

Senator TESTER. Mr. Chairman, before you leave, I have a very quick opening statement after Senator Brown, a minute. Would that be OK?

Senator BROWN. Sure.

OPENING STATEMENT OF SENATOR SHERROD BROWN

Senator BROWN. Thanks to Chairman Crapo for setting this hearing up, and welcome, Mr. Hirschhorn, Mr. Daly, and Mr. Buchanan. Thank you for your role in all of this over the years.

Congress passed ECRA last year, the Export Control Reform Act, to strengthen our country's ability to protect technology that is critical to our national security from being stolen by countries like China. We did that through creating a permanent statutory basis for U.S. export controls, which we passed alongside FIRRMA, and thank you, Mr. Hirschhorn, especially for your work on that, to get CFIUS more authority to look at a broader range of transactions. We passed both of these to strengthen our national security and give us stronger tools to protect ourselves from countries trying to get their hands on our most sensitive technologies.

Today, a year later, this hearing will help us to assess ECRA is being appropriately implemented and enforced and whether the system has the resources to get the job done. That oversight of implementation is a very important function of this Committee.

In ECRA, we included provisions designed to address emerging and foundational technologies. We know how fast technology changes. We know we needed tools that would evolve with those changes. Congress also wanted to make sure that the identification of these technologies remains an ongoing process and that new controls would be targeted to technologies that are considered essential to our national security.

The law also directed Federal agencies to take into account foreign development and availability of those technologies and the effect controls would have on the development of technologies within the United States. We want to protect U.S. national security priorities through tough and appropriate export controls. Ultimately, important national security and law enforcement considerations should, of course, be paramount, but kept separate from trade and economic considerations.

Unfortunately, as with its treatment of ZTE and Huawei, this Administration seems to be failing that crucial test. Although export control decisions can appear to be simple, each requires a complex policy and legal analysis, as you know, ones that evolve statutes, regulations, international commitments, intelligence and law enforcement, industrial base implications, license administration, foreign availability, and multilateral and bilateral foreign policy issues. The technologies we are looking at are often complex, and they are constantly evolving. Technology that were once sensitive become ubiquitous. Commercial technologies that are not normally sensitive can still be applied to new uses or by end-use users of concern in ways that could threaten our national security. Concerns about destinations and users and end uses vary widely and change consistently.

This, in other words, as you all know better than others, is complicated stuff, and we need to get it right.

As Commerce proceeds with its rulemaking process in emerging and foundational technologies, this Committee must ensure that Commerce hews to the standards established in ECRA. It is hard to have a conversation about export controls and emerging technologies without addressing the role that China plays in these areas.

Through its Belt and Road Initiative, its Made in China 2025 Initiative, China executes ambitious plans to develop new technology and manufacturing capabilities. It is investing heavily in artificial intelligence and 5G infrastructure. It is reported to be investing up to $10 billion in a national quantum information lab, and it is 2 years into an additive manufacturing plan to create a $3 billion industry by next year, and we see what additive manufacturing has done in places like Youngstown, Ohio, and elsewhere in this country.

China is focused on dominating the technology and manufacturing sectors in the decades to come. That should have us worried, especially when we remember China's history of using the same technologies it develops for economic purposes to also help modernize its military, a key driver of our efforts in the last couple years to update CFIUS and export controls. They should remain a focus of our executive agencies as they set controls and issue licenses under new export control laws and regulations.

China's sometimes illegal acquisition strategies require a forceful response from our Government and our allies. In that sense, the United States is not alone in the issues it faces from China. That is why as Commerce and other agencies identify and consider controls when foundational and emerging technologies, it is important that any new unilateral controls be implemented with an eye toward multilateral agreements. Multilateral controls like multilateral sanctions are much more effective if they are imposed by and with our allies and if control standards are harmonized as much as possible.

I think all of us on this Committee in both parties are concerned with the unilateral nature of so much that our country is doing internationally. This is a case where it cannot be so.

Senator Tester.

STATEMENT OF SENATOR JON TESTER

Senator TESTER. Thank you, Ranking Member Brown, and I want to thank you and the Chairman for having this hearing. Very, very quickly, I want to thank all the folks on the panel who are about to testify. I think it is interesting that there is nobody from the Administration here, and the fact is that export control reform implementation is critically important. Its impacts on national security are important. How we strike a balance between national security and export competitiveness is critically important, yet the Administration is not here for us to ask questions of.

I think this panel is great, and I think you should be here. But the Administration needs to be here to answer questions. If we are going to do our job as the legislative branch with the checks and balances, I do not think Democrats or Republicans or Independents

should tolerate the fact—and this is not the first Committee hearing this has happened to me that the Administration does not send somebody here at our request. And I will make the assumption that the Chairman and Ranking Member did request people from the Administration to be here.

Senator BROWN. Senator Tester, thank you. I will also emphasize that to Senator Crapo, to Chairman Crapo. You are right. When I mentioned in my opening statement about the importance of oversight, that always should include the people who are actually administering the laws. Not all of you—some of you have done that in the past, and your expertise is really, really important, but that is a big part of it. So thank you, Jon.

Let me introduce the three panelists, and we will begin. Mr. Hirschhorn is former Under Secretary for Industry and Security at Commerce, worked on FIRRMA, worked on ECRA. Thank you for that.

We will turn to Mr. Daly then as former Deputy Assistant Secretary for Investment Security at Treasury, and then conclude with Mr. Buchanan on behalf of the Center for Security and Emerging Technology.

Mr. Hirschhorn, begin please.

STATEMENT OF ERIC L. HIRSCHHORN, FORMER UNDER SECRETARY FOR INDUSTRY AND SECURITY, DEPARTMENT OF COMMERCE

Mr. HIRSCHHORN. Thank you, Senator Brown, Senator Toomey. It is an honor to be here.

The export control system's job is what I always describe as "the other side of the coin" from that of the Department of Defense. Defense's job is to make sure that if our soldiers must go onto the battlefield, they carry the most advanced, most reliable weapons we can give them. The job of BIS and its sister agencies is to ensure that our adversaries on that battlefield do not have the very best. That long has been the central aim of our export control system, and we seek this objective by controlling the transfer of sensitive technology to those who might employ it against our interests.

ECRA governs exports and re-exports of so-called dual-use technology, technology having recognized civilian as well as military applications, and of low-level military items. The existing control system has worked well, and ECRA will improve it further.

ECRA continues the system's traditional emphasis on military security and foreign policy. The statute also expresses a preference for multilateral over unilateral controls, as Senator Brown mentioned, and cautions against controls that will adversely affect the U.S. competitive position in global markets.

Importantly, ECRA requires the executive branch to identify and control exports of emerging and foundational technologies that are essential to the national security.

In reality, the executive branch has been controlling emerging technologies for decades. The perennial problem is that until a new technology is being applied in fairly specific ways, it is difficult to write regulations that are sufficiently precise to be meaningful. For one thing, due process requires the kind of specificity that one sees

in entries on the Commerce Control List and the U.S. Munitions List.

And beyond legal considerations, if we unilaterally control any technology too tightly, whether it is emerging or not, there is a good chance that we will drive research and development, and ultimately production as well, offshore. So the bottom line is that if and when potential military applications of a new technology begin to jell, it is those applications that we should control and do so multilaterally, if that is at all possible.

Foundational technologies are at the other end of the developmental spectrum in that it may be too late, rather than too early, to control them effectively. By definition, their uses are widespread and they typically are available outside the United States. Often, most or all export restrictions on them—unilateral as well as multilateral—have been removed or sharply curtailed.

A frequently cited example is that of semiconductors being sold to China. Yes, China is seeking cutting-edge chips for military purposes. Those chips are subject to tight, multilateral controls, however, and China cannot obtain them legally.

But China also seeks large volumes of chips and other commodities whose technology is several generations old, principally for use in consumer products in furtherance of its Made in China 2025 effort. These items, and the technology for their production, are subject to reduced controls, or even de facto decontrol, by the multilateral groups to which the United States belongs.

We can recontrol the U.S.-origin technologies unilaterally and thereby cutoff the sale of the resulting commodities, but it is far from certain that our allies would agree to do the same. China prefers U.S. technology. We know that. But if U.S.-based supplies were unavailable, China doubtless would buy elsewhere.

I am not saying we should not do this, but I do not think we should kid ourselves about how difficult it is to do it effectively.

Given where I spent 7 years until 2 years ago, I am not going to comment on particular China enforcement cases. As a general matter, though, I do not think it is sound policy to treat export controls, which are imposed for military and foreign policy reasons, as an element of our commercial trade policy to be bargained over along with sales of beef, chicken, soybeans, and the like. And it is even worse to treat the *enforcement* of export controls in that manner. It sends the wrong message to those who would violate our laws and put our country at risk. It places the lives of our uniformed men and women in jeopardy as well as undercutting our law enforcement agencies and respect for the rule of law.

So, in conclusion, I hope this Committee will do four things: give ECRA time to work, and I think it will work well; continue your valuable oversight of the export control process; ensure that existing control categories are reviewed regularly and revised to reflect changing threats as well as evolving technology; and, finally, give BIS the resources it needs to do the job that you have given it.

Thank you very much. I will be happy to hear your questions.

Senator BROWN. Thank you, Mr. Hirschhorn.

Mr. Daly, thank you for joining us.

STATEMENT OF NOVA J. DALY, FORMER DEPUTY ASSISTANT SECRETARY OF TREASURY FOR INVESTMENT SECURITY (2006–2009) AND SENIOR PUBLIC POLICY ADVISOR, WILEY REIN LLP

Mr. DALY. Excellent. Well, I want to thank Chairman Crapo and Ranking Member Brown for having me here today, Members of Committee. I am deeply honored to appear before you today and thank you for the opportunity to testify. The views I express today are my own. They do not represent my firm or any clients. And before I get into sort of the heart of the matters that this Committee is reviewing today, I wanted to applaud this Committee for passing ECRA and FIRRMA, excellent bills that will help this country better hone in and address our adversaries where they try to acquire U.S. critical technology through the means of going through a CFIUS process or otherwise. These pieces of legislation are seminal course corrections.

In terms of implementation and enforcement of ECRA, I want to applaud first off this Administration, especially Secretary Ross and Acting Under Secretary of BIS Nazak Nikakhtar, for their outstanding work and dedication to the efforts to enforce U.S. laws, protect U.S. technology, and also grow the U.S. economy. So good work has been done on implementing ECRA and BIS. BIS has issued an Advance Notice of Proposed Rulemaking identifying 14 categories of emerging technologies and has received and is evaluating over 200 comments to that.

BIS also recently announced that it is going to issue a Federal registrar on foundational technologies and will issue very soon a proposed rulemaking identifying the first subset of emerging technologies.

Since the start of 2017, BIS itself has initiated over 2,000 export control investigations, a 21-percent increase; has had 89 civil adjudications and 70 criminal prosecutions; and conducted more than 2,000 end-use checks on technology sales in more than 65 countries. So it is doing the good work.

So how to establish controls for emerging technology and foundational technologies while preserving the domestic innovation? Obviously, this is an important and surgical exercise that must be done with thorough assessments of U.S. innovation, their level of maturity in the United States and in allied nations, and also with foreign adversaries. Assessing controls requires the engagement of U.S. companies large and small and the focus of Congress for oversight.

And our U.S. allies and members of multilateral export control regimes should be willing partners. Ensuring the protection of intellectual property, broader global security, and the rule of law creates a platform of trust where innovation can flourish.

Now, while we must seek and use all our means for multilateral controls, that does not mean the United States should not take unilateral action where appropriate. However, we must preserve a system in the United States where R&D flourishes. It is critical to our innovation and our future.

Last, I also want to say that identifying emerging and foundational technologies also has effects, as the Senators have noted, to CFIUS and foreign investment reviews. Once these tech-

nologies are identified, they are going to be critical technologies for which for certain investments will require a mandatory declaration.

So to talk a little bit about the designations of ZTE and Huawei, as you know, Huawei was designated in May of 2019. The U.S. Government did so after determining that there was reasonable cause to believe that it had been involved in activities contrary to the United States national security and foreign policy interests. I have known Huawei since my time running the Committee on Foreign Investment in the United States since 2007, and so knowing Huawei then and seeing the actions it has taken since that time, I think BIS' determination was wholly appropriate.

That said, the President per his recent announcement, BIS will promptly be taking action to issue certain licenses to companies that apply, which permit transactions that pose no national security risk and are not contrary to the United States foreign policy interests.

The effort to closely scrutinize and restrict transactions with Chinese entities that pose national security risks is not limited to this Administration. This Congress has taken significant action, as noted in the National Defense Authorize Act Section 889.

So what about the effectiveness of ECRA in addressing China challenges? I believe that the ECRA-related controls will go a long way toward improving U.S. transparency and effectiveness in addressing the challenges related to China and its persistent diversion tactics. We have seen stronger enforcement have good progress. In FIRRMA itself and the passage, we have seen a decrease in China's investments in critical technology. I myself have been to California and seen first-hand Chinese involvement, government-controlled entities wanting to seek investment in our critical technology companies. It is important we address it because those entities are doing it for state purposes, not for commercial purposes.

Also with the implementation of ECRA, the U.S. policymakers will be able to better assess our vulnerabilities of our supply chains. I can tell you firsthand I have particular clients who are trying to develop and manufacture in the United States, but the supply chains to do that technology are not here anymore. We are in an extremely vulnerable position, and doing this assessment is critical and necessary to knowing where we are now and how we need to go in terms of being leaders in innovation and technology.

That said, possible legislative and oversight recommendations, in my written testimony I offer a few tools to address intellectual property theft and broader powers to deal with government-controlled transactions.

Last, and importantly, oversight by this Committee and Congress is critically important, and resources. We have big issues in front of us, and we need to put our resources to it, and having the person-power to do it critically to do it.

Thank you for the opportunity to appear before you today. I look forward to your questions.

Senator BROWN. Thank you, Mr. Daly.

Mr. Buchanan, please proceed.

STATEMENT OF BEN BUCHANAN, PH.D., ASSISTANT TEACHING PROFESSOR, SCHOOL OF FOREIGN SERVICE SENIOR FACULTY FELLOW, CENTER FOR SECURITY AND EMERGING TECHNOLOGY, GEORGETOWN UNIVERSITY

Mr. BUCHANAN. Thank you, Ranking Member Brown, for having me to testify. It is a pleasure to be here. I am an Assistant Teaching Professor at the School of Foreign Service and a Senior Faculty Fellow at the Center for Security and Emerging Technology, both at Georgetown University. My research specialty is examining how cybersecurity and artificial intelligence shape international security. As this Committee is well aware, export controls are legal tools that are applied to technology. If either the tool or the technology is not a good fit, export controls will fail.

Given the expertise of my two fellow witnesses on the nuances of the tools themselves, I believe I will be of most use to the Committee by talking about some of the technologies in play and what makes export controls comparatively more or less suitable to these technologies. As a way of opening our discussion, I will focus on artificial intelligence because I think it is one of the most central technologies in play today.

An analogy can help conceptualize AI. One can imagine two ways of teaching a child to perform a task. The first is to give very clear instructions in a language the child understands about what the task is and how it is to be done. The second is to show the child, through a series of examples, how the task works and have the child infer important rules and patterns necessary to succeed. At various points in children's education, they learn different tasks through each of these methods.

Traditional software development, and even some older versions of AI, work in a way that is similar to the first method. They rely on software developers understanding the problem in great depth and then imparting this expertise to the system. For example, in a program designed to play chess, the software developers may consult with grandmasters to understand the optimal strategies for a wide range of situations and then program those ideas into the code. Modern AI systems, known as machine learning systems, use the second method, the one involving inference. In a machine learning system, rather than receive clear instructions about how to do the task, software developers create an algorithm that determines how the system should learn. They then provide the algorithm with lots of relevant data and computational power.

There are thus three parts to a modern machine learning system: the algorithm, the data, and the computational power. Together, they form an essential triad, and it is worth examining each part of this triad for its suitability to export controls.

It is in vogue to say that data is the new oil. From data, machine learning systems infer important patterns and nuances and determine what success and failure look like. It is thus vital that the data provided to the machine learning system be plentiful and representative of the problem to be solved in all of its complexity.

A large part of the reason that companies like Google, Amazon, and Facebook are successful with the AI systems they deploy is because they aggregate gigantic amounts of data. In essence, the large data sets these companies assemble provide them with a com-

petitive advantage over others. Large companies based in other nations, such as China's Baidu, Alibaba, and Tencent, derive similar advantages from their data sets. Export controls are less valuable in managing this flow of data. This is both because companies already have an incentive and tools to secure and not share their assembled data and because export controls are comparatively ill-equipped for the task relative to other tools like classification or contracts.

Algorithms are the second part of the AI triad. These software instructions dictate how the machine learning system will learn. There are a wide variety of algorithms, each suited to different kinds of tasks, from classifying images to making predictions about housing prices, to generation new pictures of people who look real but do not actually exist. The algorithmic frontier is rich, and a great deal of progress has been made in the last 7 years.

The prevailing ethos is that, once an advance is made, researchers post it online and share it with others. In this sense, AI research is remarkably open, far more so than the fierce competition of the technology industry would normally suggest.

The experience of several decades has shown that Government efforts to control the export of computer code are usually futile. More generally, I have doubts about the suitability of our current list-based export controls, given the changing pace of technology and the movement of the algorithmic frontier.

This brings us to the last part of the triad: computing. It is easy to ignore, but it remains vitally important, perhaps prohibitively so. In the last 7 years, we have witnessed a revolution in computing power applied to machine learning. One study by the leading research lab OpenAI indicated that between 2012 and 2018, the computing power applied to top machine learning systems increased by a factor of 300,000 times; if a cell phone battery lasted 1 day in 2012 and increased at the same rate, that battery would now last 800 years.

There is much to discuss about why this increase in computing power has occurred, but the most salient factor for our purposes today is that, unlike algorithms and data, computing power is a function of hardware and not software. That is, computers are tangible products that are easier to manage, including with export controls. My judgment is that, to the degree that export controls are relevant to the problem of managing AI and other technologies such as 5G, it will be controls on this hardware component and likely on the hardware that manufactures specialized computer chips for AI.

To be clear, in order for any such controls to work, they must be conducted in many cases in a multilateral fashion with allies, given that a great deal of hardware engineering expertise is outside the United States.

I thank you again for holding this hearing, and I look forward to your questions.

Senator BROWN. Thank you, Mr. Buchanan.

We will start the questioning with Senator Toomey.

Senator TOOMEY. Thank you, Senator Brown, and thanks to the witnesses for joining us.

I think Senator Tester made the point during the course of his comments that part of the goal here must be to strike the right balance between limiting exports that would have, you know, adverse consequences for our country and maintaining our ability to sell other products around the world. And I am not sure we are getting that balance right in all cases, so I want to give you an example of a case that concerns me a bit and get the reaction of our witnesses.

Lycoming Engines is based in Pennsylvania. They are a constituent of mine, and they manufacture piston aircraft engines. They are one of America's leading manufacturers of piston aircraft engines for general aviation aircraft. And it is not a great secret to reveal that the technology at the heart of these piston engines is very old. It is many decades old. These engines and variations on them have been around for many, many decades. And it is equally unsurprising that they are shipped all around the world. Every country has some volume of general aviation aircraft in the world, and a huge percentage of these aircraft operate with Lycoming engines.

So it was interesting when folks at Lycoming sought to bid to provide these very engines on a specific project in China that involved unmanned vehicles. They determined that they had a legal obligation to get a license. They applied for the license to bid on this project, and they were rejected.

Now, it seems to me that what really makes UAVs interesting and special and dangerous potentially are things like the software and the sensors and the controls that allow them to be manipulated remotely. It is also interesting that Air China operates a fleet of Boeing jets that have vastly more sophisticated technology than any piston engine for a general aviation plane. And not only that, there are hundreds of Lycoming engines that are operating in China in manned aircraft. These very same engines, the exact same engines, they are being flown around in China. For instance, they operate the popular Cirrus SR20 aircraft, which is owned by a Chinese company that is ultimately owned by the Chinese government. All right? So a Chinese aircraft company buys these Lycoming engines every day to fly their planes.

So the idea that this very same engine cannot be sold to a Chinese company that is involved in developing UAVs, which are not—on the surface, these UAVs are described s intended to deliver packages. Anyway, it strikes me that maybe we do not have this balance right in terms of restricting technology rather than looking at application. When asked about an American company providing these engines, the folks at DOD or—I am not sure if it was DOD or Commerce that suggested an American company could not sell a screwdriver to the Chinese effort to build these UAVs.

So I just want to pose this question to our panel, starting with Mr. Hirschhorn. Are we getting the balance right when we take such a common, universally operated commodity product like this old technology piston engine and say, ah, but you cannot sell it for this purpose?

Mr. HIRSCHHORN. Well, I am not a bureaucrat anymore, so I want to try to refrain from giving you a bureaucratic answer. We are party to a 40-nation agreement called the "Missile Technology

Control Regime" that at this point, although probably it should not any longer, includes unmanned aerial vehicles. And there are two categories. If they have a certain payload weight, and can travel a certain distance, they are very tightly controlled. We also have knowledge of what is called the "civil-military joinder," namely, that China uses a lot of technology for both civil and military purposes. And since Tiananmen in 1989, we have a statutory prohibition, enacted by the Congress, on any sales of military items or items for the Chinese military. So when you put all of that together, I suspect that is Lycoming's problem.

Nevertheless, it may be that in this particular case and in one-off cases, it would not endanger our national security, but when you see the web of policies that have to be observed here, you can see why it is a problem.

Senator TOOMEY. My question is not really so much whether the decision was consistent with laws and regulation. It was more of sort of a theoretical question. Do we have it all right if this is the outcome that we get?

Mr. HIRSCHHORN. I think we largely have it right. Whether we have it right in every case I could not say. Whether we have it right in this case I could not say. I think if there is a belief that this is going to ultimately assist the Chinese military, it is our policy—and maybe it should not be our policy; that is what you all are here for—not to do anything that will assist the Chinese military or modernization of the Chinese military. That is what it is. If it is to change, I think it would be up to Congress to change it. I doubt that the Administration, this one or any one, would change it.

Senator TOOMEY. I am out of time. Thank you.

Senator BROWN. Thank you, Senator Toomey.

Mr. Hirschhorn, ECRA, as you know, requires an interagency process to include giving outside stakeholders an opportunity to comment as they further define emerging and foundational technologies. The categories of technologies listed in BIS' ANPRM are complex technical categories. They will drive global economies and national security in the coming decades.

What are the most important things BIS should consider when evaluating controls on these categories of technology?

Mr. HIRSCHHORN. Well, I think Senator Toomey's point is the best, which is getting it right, because it is very easy, even with existing technologies, to over- or under-control them. And you do not want to do either for the reasons that have been expressed by Senators and witnesses this morning.

In the work I did for 7 years on export control reform, I found the input from industry extraordinarily valuable. The Commerce Department and its sister agencies put forth proposed regulations and said to industry, How does this work? Does this work for you? Is it too broad? Are we catching things that are sold every day all over the world? Are we leaving things out that we ought to control? We did not get too much industry input on the last one, but plenty of input where we had it wrong.

I always used to say when I would speak with industry groups that, believe it or not, the Government does not always get it right on its own. So having that input, which I considered valuable, free,

and highly professional, did a great deal toward making export control reform the success I think it was. If we cannot get the input of the people who are making this stuff, who are developing this stuff, we cannot simply assume that the Government knows enough.

Senator BROWN. Does BIS have the resources it needs to address applications and enforcement and controls?

Mr. HIRSCHHORN. No, it does not. One of the things I did in my time there was to beg, borrow, and steal resources wherever I could get them, from the Congress, from other parts of the Commerce Department that maybe were a little more flush. It is——

Senator BROWN. And that is a continuing challenge?

Mr. HIRSCHHORN. BIS is one deep. It is a continuing challenge. If the engineer who reviews machine tool applications breaks his leg, you cannot go down the hall and say to the chemist, "You are going to do machine tools for the next 3 weeks." It is one deep, and it needs more resources. I think the budget is around $114 million today. It probably should be at least $130 million, maybe more.

Senator BROWN. Thank you.

Mr. Buchanan, a question for you. I will ask about the best ways to address China's cybersecurity threats. The Administration completed a 301 investigation against China in part because of its government's state-sponsored intellectual property theft and cyber espionage. As a result of the investigation, in an effort to bring China to the negotiating table, the Administration proposed—I am sorry, imposed, not proposed—imposed tariffs on $260 billion of Chinese imports. Those tariffs have been in place for a year. Trade talks with China seem to be at an impasse.

Has any of this gotten the Chinese government to change its ways with respect to cybersecurity? Do you see signs of that?

Mr. BUCHANAN. Obviously, it is hard to spot operations that are meant to be hidden, but I think it is fair to say China continues to be an aggressive actor in cyberspace and continues to hack targets in the United States as they perceive suits their national interest. And this is a pattern that has gone on for quite a period of time, and I do not see a lot of evidence that has slowed.

Senator BROWN. So answer a bit more broadly. The tariffs on some areas, it is clear to me tariffs have not changed Chinese behavior. You sort of speaking expansively make the same claim?

Mr. BUCHANAN. Yes, I think that is right. I do not claim expertise beyond cybersecurity, but I have not seen any indication that in response to tariffs Chinese hacking has diminished.

Senator BROWN. Can you dig down? Is there a way to impose these tariffs narrowly, or not so narrowly, to change Chinese behavior in cybersecurity?

Mr. BUCHANAN. I would be surprised if the Chinese hackers are responding to tariffs. My sense is those are different parts of the apparatus. A lot of the Chinese activity we have seen in the last couple years, at least in public, are particularly broad operations targeting many millions of Americans' data in a variety of organizations. That seems to be removed from the part of the calculus of the Government that would deal with tariffs.

Senator BROWN. OK. Thank you.

Senator Van Hollen.

Senator VAN HOLLEN. Thank you, Senator Brown. I thank all of you for your testimony today.

Before I ask about export matters, Mr. Buchanan, I am glad to have you here. You wrote an article in 2016—it was co-authored—about dealing with Russian interference in our elections. And you said, and I quote, that "The United States should put forth a declaratory policy on the vital importance of elections, vowing to impose costs on any state that interferes with the integrity of the process." You went on to say that the United States should "articulate a policy of deterrence through cost imposition that would be activated only if a foreign actor sought to tip an election to one candidate or introduce significant doubt as to the legitimacy of democracy."

I fully agree with that assessment. Senator Rubio and I have introduced a bipartisan bill that has bipartisan support that we are trying to get enacted before the 2020 election, which sets out a very simple proposition, you know: Mr. Putin, if you get caught interfering in our elections again, you will face swift, mandatory, and substantial penalties. Is that the kind of deterrence that you are talking about?

Mr. BUCHANAN. Yes, Senator. As I think we both agree, elections are foundational and fundamental to democracy, and my colleague Michael Sulmeyer and I warned prior to the 2016 election that it was important to make it clear to American adversaries that this is something we take seriously, something we seek to protect, and something that, should they decide to interfere, will be met with consequences. And I think your bill is a good step in that direction.

Senator VAN HOLLEN. Thank you. I am just going to renew my request to the Chairman and the Ranking Member, along with Senator Rubio, that we move forward on the DETER Act in Committee.

Let me now get to the issue of export controls, and, Mr. Hirschhorn, and I think listening to all of you, I think I am on the same page, which is, if we make a determination that something is in our national security interest, for example, if we think it is important to put Huawei on the entities list for the purpose of preventing exports that could strengthen their 5G network, if we make that conclusion as a country, then we should not then be making tradeoffs with respect to those national security interests in order to get concessions on tariffs or other trade-related issues. Would you all agree on that, starting with Mr. Hirschhorn?

Mr. HIRSCHHORN. I would agree very emphatically, and I will add that this is not unique to this Administration. On the enforcement side, it is unique. But during my service in the Obama administration, there were always temptations to put export control issues, national security issues on the table as part of trade negotiations, and I resisted them successfully. It looks like the resistance has not been so successful lately.

Senator VAN HOLLEN. Would you all agree with that, though, that we should not be trading off national security interests for some kind of concessions on tariffs or a trade issue?

Mr. DALY. National security is also economic security. The stronger our economy is, the stronger we are as a Nation, the more we are able to provide for our military and our national security

defenses. So having worked in the National Security Council, I saw the panoply of issues that come before a President and come before an Administration. So, broadly speaking, as long as we are pursuing our goal of national security, addressing the economic issues is important, too.

Senator VAN HOLLEN. Mr. Buchanan.

Mr. BUCHANAN. I would agree, Senator. I think we should not tradeoff between these two goals. I appreciate that there is overlap, but I think enforcement that seems to vary with the tenor of trade talks undermines the credibility of that enforcement.

Senator VAN HOLLEN. Well, let me just give everyone some examples. The President about a year ago—I should say Secretary Ross put ZTE—he put a blocking order on ZTE and stated that this was in the national security interest of the United States because ZTE had violated Iran sanctions. Within a short period of time, the President tweeted out, "I am going to remove ZTE from the blocking list because my friend President Xi as me to." Example number one.

Number two Huawei, two examples. One, Huawei was also found to be in violation of sanctions, and as a result, we have asked the Canadians to arrest the CFO of Huawei. And then the President says that he would intervene in the arrest of Huawei's CFO Sabrina Meng Wanzhou if it helps secure a trade deal with China.

Now, in my view, this is a perfect example, Mr. Hirschhorn, of what you say is dangerous, because this undermines the rule of law. If we are going to arrest somebody because they violated U.S. law, in my view—and I am asking for your opinion—it is very worrisome, risky, and counterproductive for the President of the United States to suggest that he is going to release somebody if he gets a deal or a concession on trade. Would you agree with that?

Mr. HIRSCHHORN. I agree with that emphatically. There are plenty of things that are trade related that can be put on the table. Law enforcement and national security do not belong there.

Senator VAN HOLLEN. Let me just say, Mr. Chairman, look, I agree with a lot of the efforts this Administration is taking with respect to addressing Chinese theft of technology and the national security part. I agree with their Huawei policy. But it is very, very scary to start trading off national security issues and the rule of law and arresting people with respect to trade. It is a recipe for getting other countries to grab Americans and detain and arrest them as part of an effort to extract trade concessions from the United States. Very dangerous, and I hope we will all agree that it is a bad idea.

Thank you.

Chairman CRAPO. [Presiding.] Thank you.

Senator Jones.

Senator JONES. Thank you, Mr. Chairman.

You know, Mr. Chairman, I am so tempted to follow on this and talk about how or whether or not all the Mercedes Benz and BMWs and Nissans and Toyotas are a threat to national security here, but I am going to resist the urge. I have got plenty of time to do that in other forums, I think.

So what I do want to talk to the panel about—and thank you all for being here. I apologize for being late. The higher education sys-

tem in my State of Alabama are among the universities that are leading the way in emerging technologies and specifically nanotechnology. The University of Alabama in Birmingham has a Center for Nanoscale Materials and Biointegration, and they dive into the uses of nanotechnology and how it can be manipulated for commercial use.

Now, the results of this can transform medical care we receive but also military flights. So I do not want them to get in trouble. It is a very sensitive issue. So for each of you, if you could address a little bit how is the Commerce Department and the Federal Government working with these universities and other education systems so that they can seamlessly and effectively navigate the export control laws? I will leave that to anybody.

Mr. HIRSCHHORN. I will give you 30 seconds on it. The Export Administration Regulations have for many years excluded from coverage teaching in catalogue courses by universities and associated labs. Moreover, fundamental research is not covered by the export control laws. There are a lot of people who disagree with that. There is some suggestion that there is a First Amendment need for it. But it is the work of graduate students on funded projects that really is where there are problems, and the Federal Government in my experience is quite willing to work with universities. I think universities are not always as willing to work with the Federal Government. I think some of them tend to view export controls as rules for for-profit businesses and not for universities. I think there should be closer coordination between universities and the Federal Government to make sure that, as you say, they do not get themselves in trouble.

Senator JONES. Right. Anybody want to add anything, either of you?

Mr. DALY. Yeah, I just think it is critically important to understand that there are state-led actors who would seek to get this point of the spear critical technology, nanotechnology, and bring it back to their own home country. So being extremely aware of who is involved in what studies and involved in what projects and who is funding what research is important. So it is important not only for the continuation of the great things that are happening in that university and their innovation capacity, but also making sure they have control of it for the long term.

Senator JONES. OK. So let me move on to something else that I have been very involved in with Members of this Committee, and that is trying to update our anti-money-laundering laws throughout the systems. In particular, we have been working with Senators Warner and Cotton and Rounds involving beneficial ownership, which is a real problem when you are trying to trace back funds, whether it is in human trafficking, drugs, or whatever.

So as it pertains to the export control laws, I can also see where there would be problems with entities who we do not really know who they are being controlled. How often in your experiences have you seen firms try to hide their true ownership in attempts to evade the export control restrictions? And are there strategies that we can employ? What are they doing? What can we do better? How can we tighten that up if it is a problem?

Mr. DALY. Sure. Yeah, thank you, Senator, for that question. It is an excellent one. In the private sector, I have seen that occur and also in the course of reviews by the Committee on Foreign Investment in the United States. Certainly there are in many attempts to obfuscate ownership and control, and, thankfully, we have intelligence services here in the United States, DNI and 15 other intelligence agencies that can collectively be able to identify who is actually in control and what levers they are utilizing to either control U.S. industries or gain information.

Senator JONES. Have you seen the bill that we have got pending right now and how the data would be collected and maintained? Have you had a chance to look at that?

Mr. DALY. I have not been able to, but I look forward to doing it.

Senator JONES. OK. If you would, just take a look at it and see if there is something that particularly we might need to tweak a little bit as it pertains to, you know, imports and exports to try to help better do this. I would appreciate that.

Mr. DALY. Absolutely, Senator.

Senator JONES. Awesome. Thank you, sir.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you, Senator Jones.

And to the witnesses, again, I apologize for having to slip out earlier. I had to go defend the Banking Committee's jurisdiction—which we successfully did, by the way.

Let me just conclude the hearing here with a few questions. My first one is for you, Mr. Hirschhorn. Traditionally, our export control system has—and I apologize also if this has already been covered by the other questions you have been asked. But, traditionally, our export control system has focused on national security and foreign policy. Should we expand the focus of our controls to address issues of economic competitiveness, for example, things like the Made In China 2025 Initiative?

Mr. HIRSCHHORN. It is tempting. Certainly in the last 75 years since World War II, our export control system has been focused on three things: national security and foreign policy in terms of the philosophy, but also multilateralism, which is essential for effectiveness. And many times our allies as well as our adversaries have said, "Oh, you really just want to impose these controls so you get an economic competitive advantage." We have truthfully denied that. Administrations of both parties over many decades—and I have been involved in this area for 40 years—have truthfully denied that. If we are going to expand export controls to cover economic issues and economic competitiveness, we are going to have a much harder time convincing our allies, who are essential to making any controls work, to go along with us.

So it is a difficult problem. It is a real dilemma.

Chairman CRAPO. Thank you.

Mr. Daly, do you have a thought on that?

Mr. DALY. I think we are in a singular period in time where we have to address China. So if you look at the emerging technology categories, the 14 categories, in many ways they mirror China's 2025 strategy of category of industry. So I agree with the Honorable Mr. Hirschhorn that we do have to engage and seek multilat-

eral efforts to do it. But we have to focus on addressing what China is seeking to do and what that means to our innovation and innovative capacity well in the future, not only for our companies but for the militaries they also provide.

Chairman CRAPO. All right. Thank you. And, again, Mr. Daly, China engages in unfair trade practices and it artificially subsidizes its companies in order to overdevelop and overproduce in key sectors such as semiconductors in order to dominate the world marketplace.

In order to protect the economic viability of U.S. companies, some propose that we should use export control rules to cutoff the flow of basic commercial technology that the Chinese need to compete against our companies, even if the technology has nothing to do with these, as we have been talking, the foreign national security.

Now, my question is: If we take this approach that we have been talking about, what is to prevent a non-U.S. company such as Europe or Japan from simply filling in behind? And we have seen this issue raised in the semiconductor world recently in terms of our reactions to China. Again, is the answer simply that we must work in coalition with our allies before we engage in this type of export control? Or is there some other aspect of this that we could utilize?

Mr. DALY. Yes, Senator, that is an excellent question, and it goes to the whole heart of ECRA and the purpose of it and getting the balance right in terms of protecting national security and ensuring economic growth.

Certainly engaging with our multilateral partners to come up with a combined agreement on what we should and should not export is critical to those efforts and should be ultimately fully pursued.

You know, interestingly enough, too, one of the issues to really focus on here is why is the supply chain being juggernauted in one particular area? Why does it require us providing that good in one country? Why aren't there other opportunities and other places to be able to sell that where we can have a more balanced equation and less concern about longer-term national security issues? So I think that is another consumer we have to take upon is: What have we allowed our supply chain to be held by?

Chairman CRAPO. Thank you.

And, Mr. Hirschhorn or Dr. Buchanan, do either of you have anything further on this issue you would like to say?

Mr. HIRSCHHORN. No. I think Mr. Daly has stated it well. I think that ECRA is right in stressing multilateralism. I once heard someone say that unilateral controls are like damming half a river, and I do not think it is a place we should go except in special circumstances.

Chairman CRAPO. Dr. Buchanan?

Mr. BUCHANAN. I think my colleagues have covered it well.

Chairman CRAPO. All right. Thank you.

My next question then is for you, Dr. Buchanan, and I want to kind of move into big data. I know that this is a little off topic, but the Banking Committee has been dealing with the big data issue and on a very broad basis. We have held three hearings on privacy in that zone, including on how data is used to segment, score, or

otherwise make predictions about individuals' creditworthiness, employability, or general reputation.

AI is at the center of this discussion, and I am concerned with the extent to which individuals' data is collected and processed without their knowledge, consent, or any real understanding of its scope. I believe individuals should have rights over their data similar to those that Europe in the GDPR has established, including access, control, the ability to correct, and the ability to delete.

How do AI systems complicate or challenge the ability of individuals to exercise data rights?

Mr. BUCHANAN. Well, AI systems excel at processing large amounts of data, so they increase the incentives for corporations and other organizations to try to collect that data because then they can make better use of it with such systems. They can process it at a scale that otherwise would be quite difficult.

I think it is fair to say that machine learning technology is at the core of many of the major tech companies in the world today as a result of this. So there is a greater incentive to collect the data if you can do more with it, and AI systems enable better slicing and dicing of data.

Chairman CRAPO. And in order to protect individuals' rights or essentially enhance individuals' rights to control that I would like to see us give them over their own personal data, are there things that we could do or should do legislatively—that we could do legislatively that would help to mitigate this ability of AI to overcome those rights?

Mr. BUCHANAN. Sure. I think it is important that users have not just some kind of abstract legal consent to something, but they have a meaningful understanding of how their data is being used by companies that collect it, which companies are collecting it, what they do with it.

One example of something that probably deserves—probably is not on the mind of many Americans is that as data is collected, even if the data itself is not sold or shared, inferences from that data can be—so there is a lot of nuance on the technology there, again, in part enabled by machine learning systems' ability to parse large amounts of data. And my sense is that many Americans do not have a good sense of how that all works. So meaningful consent to data use certainly would be a good thing.

Chairman CRAPO. And that would be including the management of the data as well as the sale of the data as well.

Mr. BUCHANAN. That is exactly right, the management of the data, the security of the data, and also how inferences from that data are sold or shared for ad targeting, for example.

Chairman CRAPO. All right. Thank you. Then one last question, and I will give—this is also for Mr. Buchanan, but I will give Mr. Daly and Mr. Hirschhorn an opportunity to comment on this if you would like. And it is still on the data issue.

Mr. Buchanan, in your testimony you described export controls as a relatively ineffective tool in stopping the export of algorithms given the rate of innovation and the fact that AI is a fairly open resource. You also identified the mass of personal and behavioral data as the competitive advantage for large technology companies as opposed to their AI system.

It would seem to me then that the data could also be a real vulnerability if, for instance, a foreign adversary were to obtain all of Google's consumer data. These companies are incentivized to secure their systems, but that may not be enough. And my question is: What comprehensive privacy controls or practices could help mitigate the risk of big data being used in this way?

Mr. BUCHANAN. I think it is important to disentangle security and privacy here. So for security, I think you are quite right to suggest that companies like Google and, indeed, many American companies that have large data sets are significant targets of foreign intelligence agencies. We have seen cases of Chinese hackers targeting Google going back almost a decade at this point. So the security of that data is definitely something that is vitally important as you suggest.

Privacy is very important, as your previous question suggested. I think it is slightly distinct insofar as there are privacy concerns that do not relate to foreign actors but relate to the companies themselves. But if your question is should we be worried about foreign intelligence agencies trying to seek access to large data sets of Americans held by American companies, the record unequivocally suggests the answer is, yes, we should be concerned.

Chairman CRAPO. Thank you.

Mr. Daly or Mr. Hirschhorn, do you have anything to add to those questions?

[Witnesses shaking heads.]

Chairman CRAPO. All right. Well, again, I want to thank you, all of you, for not only coming here today and sharing your insights and wisdom on this with us, but for the support and assistance you have given us as we deal with this issue. These are obviously becoming more and more important and critical as we move forward to deal with—the obvious example is China, but to deal with this set of issues across the globe. So I appreciate you being here today and look forward to working with you in the future.

And that brings me to this: For Senators wishing to submit questions for the record, those questions are due in 1 week, on Thursday, July 25th, and we ask that each of you respond to these questions if they come in as promptly as you can.

Again, thank you for being here. This hearing is adjourned.

[Whereupon, at 11:08 a.m., the hearing was adjourned.]

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

PREPARED STATEMENT OF CHAIRMAN MIKE CRAPO

The hearing will come to order.

No one can dispute that technological advances are of vital importance to United States progress and development, where progress in knowledge and innovations undergird the growth of U.S. economic productivity.

The U.S. China Commission found that about half the U.S. GDP and two-thirds of its productivity gains is attributable to U.S. technology improvements.

In August 2018, the President signed the Foreign Investment Review Modernization Act, called "FIRRMA," and the Export Control Reform Act, known as "ECRA" into law.

FIRRMA is designed to strengthen the existing regulatory architecture in significant ways to deal with inbound foreign investments that would have the potential to threaten U.S. national security interests.

ECRA importantly reauthorizes an otherwise moribund Export Administration Act, continued only by annual reissuances of Presidential national security declarations.

It authorizes the Bureau of Industry and Security (BIS) at Commerce to update controls on exports designed to prevent certain U.S. dual-use technologies, lower-level military items and other things from ending up in the wrong hands.

These two important, hugely bipartisan bills were intended, in no small part, to ensure that with proper controls in place to establish highly guarded inward and outbound regimes, a productive relationship between the United States and China is not only possible, but could be of the highest value in terms of global prosperity and security.

Today's hearing picks up from where the Committee left off when it last looked at assessing investment controls on technology in its June 4th hearing on "Confronting Threats from China."

On June 4th, we examined China's intention to secure global technological leadership for itself, with a particular emphasis on some of its inbound foreign direct investment strategies, particularly into the U.S. semiconductor industry.

Today, the Committee shifts gears slightly to examine control issues surrounding exports of things outbound from the United States, and other re-exports or transfers that may occur abroad.

Right now, there is a raft of export control regulation on the horizon at the Commerce Department.

So far, BIS is actively engaged on two rulemaking fronts covering "emerging and foundational technologies," which include technologies from such sectors as artificial intelligence, computing, additive manufacturing, data analytics, robotics, surveillance and a long list of others.

Importantly, items BIS designates as "emerging technology" will also be deemed to be "critical technology" under FIRRMA, and subject many potential inbound investment deals to CFIUS review notification requirements.

The current rulemaking under consideration at BIS is not set in stone.

It is busy pouring over a myriad of industry and government comments that will inform its application of strict controls over emerging technologies, which industry will use to understand to whom it can transfer these technologies, who can otherwise use them and who can even research them.

The Committee has before it a very accomplished panel of witnesses assembled to help us pull apart the underlying risks associated with the United States continuing its robust international economic relationships, including that with China, against preserving U.S. technological leadership over these emerging and foundational technologies and some of the more sensitive items that that would produce.

In the past, export controls sometimes have not been able to keep up with innovation, and this problem is exacerbated by today's pace of advancements, particularly in the 'artificial intelligence' sector, which owing to its nature is itself a difficult sector to control.

Considering that BIS is very unlikely to designate all artificial intelligence technology, we are fortunate to have Dr. Buchanan here today to help the Committee better understand what "artificial intelligence" means, how it works, and why or why not certain aspects are more controllable than others.

Our professional export control experts, Mr. Hirschhorn and Mr. Daly are expected to offer their assessments on how BIS may establish controls that address emerging and foundational technologies, while preserving the innovative capacity of the United States.

PREPARED STATEMENT OF SENATOR SHERROD BROWN

Thank you, Chairman Crapo, for holding this hearing, and thank you to our witnesses for being here today.

Last year, Congress passed ECRA, the Export Control Reform Act, which provided a permanent statutory basis for U.S. export controls, alongside and in tandem with FIRRMA, the Foreign Investment Risk Review Modernization Act, to broaden the range of transactions that the CFIUS process would assess. Both of these measures exist to serve key U.S. national security and foreign policy objectives.

Today, nearly 1 year later, this hearing will help us to assess our current export control regime and whether ECRA is being implemented and enforced in a system that is resourced to get the job done.

In ECRA, Congress included provisions designed to address emerging and foundational technologies. In crafting these provisions, Congress recognized the dynamic nature of technological innovation and the importance of control and enforcement processes that would evolve with those changes.

Congress also sought to ensure that identification of these technologies remains an ongoing and organic process, and that new controls be limited to technologies that are considered essential to U.S. national security.

It also directed Federal agencies to take into account foreign development and availability of those technologies, and the effect controls would have on the development of the technologies within the United States.

We want to protect U.S. national security priorities through tough, appropriate export controls. Ultimately, important national security and law enforcement considerations should be paramount, but kept separate from routine trade and economic considerations. Unfortunately, as with its treatment of ZTE and Huawei, this Administration seems to be failing that crucial test.

Although export control decisions can appear to be simple, each one requires complex policy and legal analyses involving statutes, regulations, international commitments, intelligence and law enforcement equities, industrial base implications, license administration, foreign availability, and multilateral and bilateral foreign policy issues.

The technologies are often complex and evolving. Technologies that were once sensitive become ubiquitous. Generally nonsensitive commercial technologies can be applied to new uses or by end users of concern in ways that can harm our interests. Concerns about destinations, end users, and end uses vary widely and change constantly. This is, in other words, complicated stuff. And we must get it right.

As Commerce proceeds with its rulemaking process on emerging and foundational technologies, this Committee must ensure that Commerce hews to the standards established in ECRA.

It's hard to have a conversation about export controls and emerging technologies without addressing the role China plays in these areas.

Through its Belt and Road Initiative and Made in China 2025 initiative, China is executing ambitious plans to develop new technology and manufacturing capabilities. It is investing in artificial intelligence and 5G infrastructure. It is reported to be investing $10 billion in a national quantum information lab. And it is 2 years into an additive manufacturing plan to create a $3 billion industry by next year.

China is laser-focused on dominating technology and manufacturing sectors in the decades to come. China's history of diversion of dual-use items to help modernize its military and its civil-military fusion policies were a key driver of our efforts to update CFIUS and export controls last year. They should remain a focus of our executive agencies as they set controls and issue licenses under new export control laws and regulations.

China's sometimes illegal acquisition strategies require a forceful response from the U.S. Government and our international allies. In that sense, the United States is not alone in the issues it faces from China.

That's why, as Commerce and other agencies identify and consider controls on emerging and foundational technologies, it's important that any new unilateral controls be implemented with an eye toward multilateral agreements.

Multilateral controls—like multilateral sanctions—are much more effective if they are imposed by and with our allies, and if control standards are harmonized to the degree they can be.

Thank you. I look forward to hearing from our witnesses.

PREPARED STATEMENT OF ERIC L. HIRSCHHORN

FORMER UNDER SECRETARY FOR INDUSTRY AND SECURITY
DEPARTMENT OF COMMERCE

JULY 18, 2019

Chairman Crapo, Ranking Member Brown, and Members of the Committee, I am honored to be asked to share my thoughts on a number of critical current issues in U.S. export controls. My involvement in the field spans more than 40 years and includes service in the Administrations of Jimmy Carter and Barack Obama, with three decades of private law practice in between. Although I provide some export control assistance to private clients these days, my comments here reflect my personal opinions only.

The Chairman's invitation requests my "assessment of current implementation and enforcement of ECRA, including related regulations, and how the United States may establish controls that address emerging and foundational technologies while preserving domestic innovation," as well as my thoughts about "recent designations of ZTE, Huawei, and other Chinese technology companies" and, "[w]ith respect to China, including the persistent diversion challenges it poses, [my] perspectives on whether . . . emerging ECRA-related control structures in the United States will be effective in confronting these challenges." Finally, you ask for "any other legislative or oversight recommendations" I might have to offer. I will do my best to respond to each of these requests.

When I had the honor of serving as head of the Bureau of Industry and Security, I often described BIS' job as being the other side of the coin from that of the Department of Defense. DOD's job is to ensure that if our soldiers have to go onto the battlefield, they carry the most advanced, most reliable weapons and other equipment that we can give them. The job of BIS and its sister agencies is to ensure that our adversaries on that battlefield do *not* have the very best. That long has been the central aim of our export control system.

We seek this objective by controlling the transfer of sensitive technology to those who might employ it against our interests. The Export Control Reform Act—ECRA—wisely points out, though, that the imposition of controls should come "only after full consideration of the impact on the economy"[1] and on U.S. competitiveness in global markets,[2] as well as consideration of whether the technology in question is "widely available from foreign sources."[3]

Let me note parenthetically that in my 40 years of involvement with export controls, I have observed that although there can be vigorous disagreements about control policies, individual licenses, and the like, the disputes are decidedly *not* partisan. The Obama administration's Export Control Reform initiative offers a good example. Some Democrats criticized what we were doing and many Republicans were supportive. Indeed, the chairman of the House Foreign Affairs Committee, a long serving Republican Member, complained to me at one point that we were not moving quickly enough.

ECRA Implementation and Enforcement

ECRA was enacted last August. Like most statutes that address ongoing issues, it does not have an expiration date. This means that its passage ended a decades-long pattern in which the Export Administration Act of 1979 would expire, the President would continue the Commerce Department's export control authorities under the International Emergency Economic Powers Act, renewing the authorities annually, until Congress revived the Export Administration Act, the export act would expire again, and the pattern would repeat itself.

ECRA relates to exports *from* the United States, as well as to subsequent reexports and transfers abroad. It establishes a control system for so-called dual use items—those having recognized civilian as well as military applications—and low-level military items. That system is administered by the Department of Commerce in consultation with the Departments of Defense, State, and Energy.

ECRA was enacted with a companion statute called the Foreign Investment Risk Review Modernization Act, or FIRRMA, which amends the process for reviewing foreign investments that are *inbound* into the United States.[4] The inbound invest-

---

[1] Export Control Reform Act of 2018 (ECRA), Pub. L. No. 115–232, § 1752(1), 132 Stat. 2210 (codified at 50 U.S.C. § 4811(1)).
[2] ECRA § 1752(3) (codified at 50 U.S.C. § 4811(3)).
[3] ECRA § 1752(6) (codified at 50 U.S.C. § 4811(6)).
[4] Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), Pub. L. No. 115–232, § § 1701–1728, 132 Stat. 2174.

ment review is conducted by CFIUS—the Committee on Foreign Investment in the United States. One goal of the CFIUS process, which also is a long time goal of the export control system, is to ensure that a foreign person who invests in the United States will not thereby gain access to technology that we would not allow to be exported directly to his or her home country.

The original FIRRMA legislation would have directed CFIUS to draw up a sensitive technologies list that would have been similar, but not identical, to the lists that already are part of the existing export control system. I and others ultimately convinced the sponsors of the FIRRMA bill that rather than have a body without export control expertise set up a potentially duplicative list, the measure should strengthen the existing export control system. Given the already-felt need of many in Congress to enact permanent export control legislation, Congress sensibly came up with ECRA as the solution.

What does ECRA do? To a considerable degree, it codifies the existing Commerce Department control mechanism, including the changes made by the Export Control Reform initiative. For that reason, ECRA requires few substantive regulatory changes aside from those involving emerging and foundational technologies, which I'll address in a moment.

ECRA sets out a statement of policy that continues the traditional emphasis on military security and foreign policy, including prevention of the proliferation of weapons of mass destruction, strengthening our defense industrial base, and focusing controls "on those core technologies and other items that are capable of being used to pose a serious national security threat to the United States."[5] It also expresses a preference for multilateral controls over unilateral controls, cautions against control measures that will adversely affect the U.S. competitive position in global markets, calls for regular updates of U.S. controls, encourages strong enforcement, and notes the complementarity of the export control and CFIUS processes in "controlling the transfer of critical technologies to . . . foreign persons."[6]

Substantively, ECRA continues in force the broad existing powers of the Commerce Department to administer and enforce controls on exports of dual-use and lower-level military items, as well as restrictions on activities of U.S. persons in support of foreign military and intelligence activities.[7] ECRA also clarifies and expands considerably the tools available to BIS' Office of Export Enforcement.[8]

ECRA requires that licensing decisions take into account whether denial of a proposed export will have a significant negative effect on the U.S. defense industrial base, as well as whether approval would engender "significant production of items relevant for the defense industrial base outside the United States."[9]

Emerging and Foundational Technologies

ECRA requires the executive branch to identify, and the Commerce Department to control exports of, "emerging and foundational technologies that . . . are essential to the national security of the United States" and are not already controlled under one of our existing export control programs.[10] The statute directs that this effort take into account such criteria as national security, foreign availability, whether a unilateral control would harm domestic research and innovation, the effect on our defense industrial base, and the willingness of our allies to impose similar restrictions. For a host of reasons, I am uncertain whether this exercise will yield significant results.

The Commerce Department has thus far taken two initial regulatory steps in carrying out this mission. First, an Advance Notice of Proposed Rulemaking (ANPRM), seeking comments on possible emerging technology controls, was published in November 2018.[11] The comment period closed in January and a substantial number of comments were received. I'm told that further action on that rulemaking, as well as on a companion ANPRM on foundational technologies, was delayed substantially by the Government shutdown earlier this year but that progress is being made on both fronts.

Second, BIS promulgated a number of new and revised export controls on emerging technology items in May.[12] These had been agreed to in the Wassenaar Arrangement, which is a group of about 40 countries that agree upon and then implement "national security" controls. Strictly speaking, the controls promulgated in May

---

[5] ECRA § 1752(1)–(2) (codified at 50 U.S.C. § 4811(1)–(2)).
[6] ECRA § 1752(3)–(10) (codified at 50 U.S.C. § 4811(3)–(10)).
[7] ECRA § 1753 (codified at 50 U.S.C. § 4812).
[8] ECRA § § 1754(a)(10), 1761 (codified at 50 U.S.C. § § 4813(a)(10), 4820).
[9] ECRA § 1756(d) (codified at 50 U.S.C. § 4815(d)).
[10] ECRA § 1758 (codified at 50 U.S.C. § 4817).
[11] 83 Fed. Reg. 58201 (Nov. 19, 2018).
[12] 84 Fed. Reg. 23886 (May 23, 2019).

aren't within the new procedural framework established by ECRA but I suspect they are indicative of the kinds of controls we will see on emerging technologies.

Emerging technologies. I agree wholeheartedly that we should impose appropriate controls on emerging technologies with national security implications and should do so as early in their development as practicable. Indeed, that is what the executive branch has been doing for decades. For controls to be truly effective, they should be adopted by our allies in the four multilateral export control regimes as well as unilaterally by the United States.[13]

The principal problem with regulating an emerging technology is that until it is being applied in fairly specific ways, it's difficult to write regulations that are sufficiently precise to be meaningful to regulators and exporters. By way of example, the Commerce Department can't very well promulgate a regulation that just says, "Don't send advanced materials technology to China" unless that regulation sets out particular applications and technical parameters. A general or generic prohibition isn't specific enough to inform exporters what can and cannot be sent to China, or to tell enforcement agents, prosecutors, judges, or juries when an exporter has broken the law.

Less than a month ago, the Supreme Court reminded us that "[i]n our constitutional order, a vague law is no law at all"[14] and that "[v]ague laws contravene the first essential of due process of law that statutes must give people of common intelligence fair notice of what the law demands of them."[15] In short, due process requires that a regulation set out clearly and specifically the boundary between what is lawful and what is not. That in turn requires the kind of specificity that one sees in entries on the Commerce Control List and the U.S. Munitions List.

And beyond due process considerations, if we unilaterally control *any* technology too tightly, whether it's emerging or well on the way to being in common use, there's a good chance that we will drive research and development, and ultimately production as well, offshore. This is not idle speculation, as we have seen very tight U.S. export controls engender the development of foreign competition in such sectors as machine tools, commercial space, and commercial thermal imaging.

Further, we saw in the course of Export Control Reform how important it is to seek private sector input on proposed controls. The Government's technical experts are knowledgeable but they don't always have full information on what currently is available in the global marketplace. Input from industry helped ensure that our rules, when published in final form, neither over-controlled nor under-controlled the technologies in question.

So when it comes to controlling emerging technologies, the sensible approach is for the Government to do what it already has been doing for decades and what ECRA is telling it to do now: Follow emerging technologies, with a particular eye toward applications that would give an adversary a military or intelligence advantage. If and when those potential applications begin to become concrete (and hence to be suitable subjects for legally enforceable regulation), control those—if at all possible, in the context of the multilateral export control groups rather than unilaterally. Securing agreement for multilateral control is difficult, time-consuming work but it is the most promising route to success.

Foundational technologies. In a sense, foundational technologies are at the opposite end of the developmental spectrum from emerging technologies. The problem with an emerging technology is that it can be too *soon* to control it if specifics are not available. The problem with foundational technologies, by contrast, is that it may be too *late* to control them effectively. By definition, their uses are widespread—so much so that they're well known and typically available from numerous sources outside the United States. In many instances, most or all export restrictions on them—unilateral as well as multilateral—have been lifted or sharply curtailed.

A frequently cited example is that of semiconductors being exported to China. Yes, China would love to get its hands on cutting-edge chips and use them for military purposes. Those high-end chips are subject to tight, multilateral export controls, however, and China cannot obtain them legally.

But China *also* is very happy to buy large volumes of chips and other commodities whose technology is several generations old, for use in consumer products in furtherance of its Made in China 2025 effort. These items, and the technology needed for their production, no longer are viewed as having significant military utility and so are subject to reduced controls, or even de facto decontrol, by the multilateral groups to which the United States belongs. The United States presumably can re-

---

[13] In addition to the Wassenaar Arrangement, these are the Nuclear Suppliers Group, the Australia Group (chemical and biological weapons), and the Missile Technology Control Regime.

[14] United States v. Davis, 139 S. Ct. 2319, 2323 (2019) (Gorsuch, J.).

[15] *Id.* at 2325 (interior quotation marks omitted).

control the U.S.-origin technologies and cutoff the sale of the resulting commodities to China but it's far from certain that our allies would agree to do the same. China would prefer to purchase the products that use U.S. technology because they know that our goods are the most reliable, but if U.S.-based supplies were to become unavailable, China would shift its purchases to other sources.

The problem with controlling foundational technologies, then, is their ubiquity. Simply put, the United States ordinarily isn't the only potential source, so preventing China from acquiring these items made here or based on our technology may hurt U.S. companies, U.S. workers, and our overall defense industrial base more than it impairs the Chinese effort to dominate us economically.

Underlying the idea of restricting foundational technology exports is the longstanding question whether export controls should be used to address only concerns about military security and foreign policy or should be expanded to address concerns about economic security or economic competitiveness. Since the end of World War II, U.S. export controls have been focused on military and foreign policy concerns. ECRA continues this approach, stating in section 1752(1)[16] that export controls should be focused on contributions to the military potential of possible adversaries and on furthering the foreign policy of the United States.

Other countries, including not only adversaries but also some of our closest friends, have voiced suspicions over the years that our controls are intended to advance U.S. commercial and economic goals. Successive U.S. Administrations of both parties—truthfully, in my view—have denied this forcefully. Although the focus of our controls could be expanded, doing so would represent a sharp break from past policy, would be inconsistent with the ECRA legislation that Congress passed less than a year ago, and would make it more difficult to convince our allies to follow our lead.

China Enforcement Issues

During my time in the Obama administration, I was involved in the development of the Commerce Department case against ZTE. I also was aware of the beginnings of Commerce's Huawei investigation. I think it best to avoid specific comments on these two matters or other individual cases that were pending during my tenure. I will comment, though, on the high degree of professionalism among BIS' enforcement agents and lawyers. I cannot imagine that the cases they developed against these or any other defendants were politically motivated or otherwise not strictly "by the book." They may not always be right but their motivations are bona fide.

As a policy matter, I don't think it's a sound idea to treat export controls—which are imposed for military security and foreign policy reasons—as an element of our commercial trade policy, to be bargained over along with sales of beef, chicken, soybeans, and the like. It is even worse to treat the enforcement of export controls in that manner.

Public horse trading of national security and law enforcement for sales of agricultural commodities sends the wrong message to those who would violate our laws and put our country at risk. Such a course of action places the lives of our uniformed men and women in jeopardy as well as undercutting the mission of our law enforcement agents and public respect for the rule of law.

Other Issues

Like my friend and former Commerce colleague, Kevin Wolf, who testified here about 6 weeks ago, I think that your best course of action is fourfold.

- First, give ECRA time to work—and I expect that it will work well.
- Second, continue the Committee's valuable oversight of the export control process, including ECRA implementation.
- Third, ensure that existing control categories are reviewed regularly and, with industry input, revised to reflect changing threats as well as evolving technology development and applications.
- Finally, give BIS the resources it needs to do the job that Congress has assigned to it. This final point is important. BIS' talented and dedicated staff cannot carry out their responsibilities without adequate resources. The budget was too small when I was there and the substantial workload increase since then has greatly outstripped the modest resource increase that has accompanied it. Do not starve this valuable operation, which punches far above its weight.

Thank you again for your interest in this important topic. I'd be glad to respond to any questions the Committee may have.

---

[16] Codified at 50 U.S.C. § 4811(1).

PREPARED STATEMENT OF NOVA J. DALY

FORMER DEPUTY ASSISTANT SECRETARY OF TREASURY FOR INVESTMENT SECURITY (2006–2009)
SENIOR PUBLIC POLICY ADVISOR, WILEY REIN LLP

JULY 18, 2019

Chairman Crapo, Ranking Member Brown, and Members of the Committee, I am honored to appear before you today and thank you for the opportunity to testify. The views I express today are my own and do not reflect those of my firm, Wiley Rein LLP, nor any client. My views are based on my over 20 years of experience in and outside of Government. They include service at the U.S. Treasury Department administering the Committee on Foreign Investment in the United States (CFIUS), at the National Security Council, on the Senate Finance Committee, and in other positions at the U.S. Department of Commerce, as well as work in the private sector addressing trade, export control, sanctions, foreign investment and multiple national security matters. Again, thank you for the opportunity to testify.

My testimony today will address five matters that this Committee is exploring regarding the implementation of U.S. export control reforms, notably those under the Export Control Reform Act of 2018 (ECRA).[1] My presentation:

I. Provides an assessment of the current implementation and enforcement of ECRA, including related regulations;

II. Describes how the United States may establish controls that address emerging and foundational technologies while preserving domestic innovation;

III. Addresses recent designations of Zhongxing Telecommunications Equipment Corporation (ZTE), Huawei Technologies Co. Ltd. (Huawei), and other Chinese technology companies;

IV. Discusses whether ECRA-related control structures in the United States will be effective in confronting the challenges raised with respect to China, including the persistent diversion challenges China evokes; and

V. Proposes possible legislative or oversight recommendations regarding the topics covered today.

Before addressing these matters, I want to applaud this Committee for its work in passing ECRA as well as the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).[2] These two pieces of legislation are historic and seminal "course corrections," providing the United States with the ability to address the actions of adversarial powers and persons more adroitly and comprehensively in a world where economic and cyber security and technological leadership are pivotal to core and peripheral U.S. national and economic security considerations as well as global peace and order.

I. Assessment of Current Implementation and Enforcement of ECRA, including Related Regulations

In order to appropriately frame this topic, it's important to take account of the accomplishments of this Administration and Congress that have been undertaken to address U.S. economic and national security vulnerabilities. These include the development and passage of ECRA, FIRRMA, provisions within the National Defense Authorization Act for Fiscal Year 2019 (NDAA),[3] addressing telecommunication and video surveillance vulnerabilities, Section 232 investigations under the authority of the Trade Expansion Act of 1962, increased enforcement activities by BIS, and executive orders (E.O.) on supply chain security[4] as well as those that seek to stimulate U.S. manufacturing and job growth. I applaud the leadership of Senator Crapo in this Committee in passing multiple national security legislative actions and oversight, as well as that of Senator Brown, including his proposed bill to safeguard matters impacting economic and national security.

As Commerce Secretary Wilber Ross recently noted, "[e]conomic security is essential to national security" and safeguarding our technology "is not easy, since the

[1] Subtitle B, Part 1, P.L. 115–232.
[2] Title XVII, P.L. 115–232.
[3] P.L No: 115–232.
[4] E.O. 13873, "Securing the Information and Communications Technology and Services Supply Chain."

boundaries between civilian and military technologies become ever more narrow as technologies are increasingly omnipresent."[5]

The efforts of this Administration, and specifically Secretary Ross and acting Under Secretary for the Bureau of Industry and Security (BIS) Nazak Nikakhtar are to be greatly lauded and supported. Given the tasks before them[6] and the degree of increased vulnerabilities to U.S. technology, infrastructure and innovation, it is critical that additional resources and support be provided to safeguard U.S. national security and ensure the rapid implementation of new programs.

Focusing on the implementation of ECRA, on November 19, 2018, BIS issued an Advance Notice of Proposed Rulemaking (ANPRM) requesting public comment on identifying 14 categories of "emerging technology." The full list of emerging technologies that BIS identified is available at: *https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.*[7]

As BIS relayed, the categories of emerging technology were provided for illustrative purposes and comments to them were not restricted just to those categories. BIS noted further that any controls on identified emerging technologies would not apply broadly to the general categories listed in the ANPRM, but rather on a narrow and meaningful subset of those categories.

The ANPRM summarized BIS' objective as follows:

> *As controls on exports of technology are a key component of the effort to protect sensitive U.S. technology, many sensitive technologies are listed on the Commerce Control List (CCL), often consistent with the lists maintained by the multilateral export control regimes of which the United States is a member. Certain technologies, however, may not yet be listed on the CCL or controlled multilaterally because they are emerging technologies. As such, they have not yet been evaluated for their national security impacts. This advance notice of proposed rulemaking (ANPRM) seeks public comment on criteria for identifying emerging technologies that are essential to U.S. national security, for example because they have potential conventional weapons, intelligence collection, weapons of mass destruction, or terrorist applications or could provide the United States with a qualitative military or intelligence advantage. Comment on this ANPRM will help inform the interagency process to identify and describe such emerging technologies. This interagency process is anticipated to result in proposed rules for new Export Control Classification Numbers (ECCNs) on the CCL.*
>
> *Commerce does not seek to expand jurisdiction over technologies that are not currently subject to the Export Administration Regulations (EAR), such as "fundamental research" described in § 734.8 of the EAR. For purposes of this ANPRM, Commerce does not seek to alter existing controls on technology already specifically described in the CCL. Such controls would generally continue to be addressed through multilateral regimes or interagency reviews.*

Following the issuance of the ANPRM, I understand that BIS received just over 230 comments and is currently evaluating them and working through an interagency process to identify controls, where warranted.

BIS recently announced that an ANPRM for "foundational" technologies will be issued very soon, and that a proposed rule identifying a first subset of controls on "emerging" technologies will be forthcoming as well. Further, BIS has emphasized throughout this regulatory process that the controls that will be implemented will be thoughtful, targeted, and focused on "choke points," as opposed to broad, blanket controls on technologies initially identified in the ANPRM process. BIS has emphasized the critical importance of industry input, and that it is taking into account all of the comments that have been submitted on emerging technologies.

BIS has additionally made clear that achieving multilateral controls on these technologies would make the most sense and that the process of identifying and implementing controls on emerging and foundational technologies will be ongoing, consistent with BIS' normal rulemaking approach. Toward that end, it should be noted

---

[5] Remarks by U.S. Commerce Secretary Wilbur L. Ross at the Bureau of Industry and Security Annual Conference on Export Controls and Security, July 9, 2019.

[6] Since the start of 2017, BIS has initiated 2,284 export control investigations, a 21 percent increase in the number of cases opened from the previous two-and-a-half years.

[7] The list includes: 1. Biotechnology; 2. Artificial intelligence (AI); 3. Position, Navigation and Timing (PNT) technology; 4. Microprocessor technology; 5. Advanced computing technology; 6. Data analytics technology; 7. Quantum information and sensing technology; 8. Logistics technology; 9. Additive manufacturing (*e.g.,* 3D printing); 10. Robotics; 11. Brain-computer interfaces; 12. Hypersonics; 13. Advanced Materials; and 14. Advanced surveillance technologies.

that as a result of a Wassenaar Plenary in 2018, in May 2019, BIS published a final rule that revises the CCL to implement certain changes made to the Wassenaar Arrangement List of Dual-Use Goods and Technologies maintained and agreed to by governments participating in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (Wassenaar Arrangement).[8]

Taking on this mandate under the ECRA is no small task. In my view, addressing these matters is one of the most critical actions this Administration will undertake, and I believe that good progress is being made given the critical nature of the efforts, the extent of industry input, and the domestic and global impact of BIS' determinations.

II. Establishing Controls that Address Emerging and Foundational Technologies While Preserving Domestic Innovation

The establishment of export controls that address emerging and foundational technologies should be a surgical exercise, and as I alluded to earlier, in my view probably one of the most important undertakings affecting U.S. technology innovation and leadership now and well into the future. The task of identifying emerging technologies is necessarily complex because these technologies are currently being developed (hence "emerging") as opposed to more mature technology (*e.g.,* foundational).

The process that BIS should and is undertaking to identify emerging technologies includes an assessment of U.S. innovation in various categories of emerging technologies, the level of maturity of these technologies in the United States and in allied nations, and foreign adversarial uses of these emerging technologies. Once BIS and its interagency partners develop a good understanding of these facts, they can better assess what types of controls, if any, make sense for particular emerging technologies with the goal of ultimately also gaining agreement on multilateral controls.

While this task requires an understanding of which technologies are broadly disseminated and which are not, it does not mean that technology which is available outside of the United States should automatically be excluded from targeted unilateral actions to control it, where appropriate.

U.S. allies and members of multilateral export control regimes should be willing partners. Ensuring the protection of intellectual property, broader global security and the rule of law creates a platform of trust where innovation can flourish. Without such a platform and without such unity, clearly the United States will need to take certain unilateral actions. It is my hope that where the United States sees a necessity to protect particular emerging and foundational technologies, our allies will step up and work with us. We should all encourage active participation and support by our allies.

Currently, the United States has four multilateral regimes for export controls: the Wassenaar Arrangement; the Australia Group; the Nuclear Suppliers Group; and the Missile Technology Control Regime. Through each of these regimes, countries identify the items to control (*i.e.,* products, software, and technology), but the controls must be implemented in national legislation. More specifically, while countries multilaterally agree on controls of specific items, all countries have divergent licensing policies on their exports, some with stringent policies restricting exports, and some with more relaxed policies. This issue can frustrate the purpose of a multilateral regime because companies facing more stringent policies in certain countries cede global market share of the controlled items to companies in countries with more relaxed policies. The resultant pressure on countries to protect market share often leads to an underutilization of export control authority. This is not to mention that the controls themselves are not effective when countries have different licensing policies.

I understand that BIS is, however, actively engaging with like-minded partners to establish a working group, at the leadership level, to discuss coordinating policies on emerging technologies so that U.S. policies of control—licensing review—are consistent across countries, and that there is better information-sharing among countries as to what items are being exported to what countries, and what items are facing broader export restrictions. Export controls need to be harmonized if they are to be effective.

---

[8] This rule added five recently developed or developing technologies (*i.e.,* emerging technologies) that are essential to the national security of the United States to the EAR's CCL, including discrete microwave transistors (a major component of wideband semiconductors), continuity of operation software, post-quantum cryptography, underwater transducers designed to operate as hydrophones, and air-launch platforms.

Addressing controls on emerging and foundational technologies also requires engagement with U.S. companies large and small, the focus of Congress to provide resources and oversight, and frankly a certain degree of patriotism. U.S. companies must be clear eyed in knowing that certain potential "business" partners actually represent the interests of foreign governments who will use their technology and know-how to the economic and military detriment of the United States and our allies.

That said, it is important that we have a system where R&D works here in the United States, but also that key technology does not leave our shores, especially where there is a national security/military nexus. Further, placing appropriate controls on emerging and foundational technologies should be undertaken to address China's "Made in China 2025" initiative. This initiative/plan emphasizes China's priorities for high-tech industries as relayed in the 13th Five Year Plan. The industries that China has identified include: 1) new advanced information technology; 2) automated machine tools & robotics; 3) aerospace and aeronautical equipment; 4) maritime equipment and high-tech shipping; 5) modern rail transport equipment; 6) new-energy vehicles and equipment; 7) power equipment; 8) agricultural equipment; 9) new materials; and 10) biopharma and advanced medical products.

Last, the identification of emerging and foundational technologies will also impact the work of CFIUS and its Pilot Program mandatory declarations. Prior to the enactment of FIRRMA, CFIUS was essentially a voluntary process, and CFIUS was authorized to review only transactions that could result in foreign control of a U.S. business. However, under FIRRMA and the Pilot Program, CFIUS is now able to review certain noncontrolling investments in U.S. critical technology companies, including any acquisition of an equity interest that affords a foreign person with access to specified information or governance rights. Transactions covered under the Pilot Program include any investment in a U.S business engaged in critical technology that operates in 1 of 27 specifically identified protected industries (Pilot Program Industries). If a transaction is covered by the Pilot Program, failure to file a "declaration" or a full CFIUS notice 45 days prior to completion of the transaction could result in civil penalties up to the value of the transaction. Once identified by BIS, emerging and foundational technologies will also be considered critical technologies for the purpose of mandatory CFIUS declarations.

While at Treasury running the CFIUS process, I saw first-hand the limitations of the voluntary process where actors acquired new and critical technologies outside of CFIUS' purview. Now with ECRA and FIRRMA, we can better safeguard the loss of our critical technologies (including emerging and foundational technologies) to those who would do harm to our economic and national security. Since my service in Government, I have observed an increasing number of transactions involving Chinese parties where the technology at issue could be viewed to present a lower threat, but the actual threat posed by the transaction related to vulnerabilities in the U.S. supply chain. Such vulnerabilities augment the ability of rogue actors to leverage the U.S. supply chain thereby raising national security concerns, including: undercutting direct competitors; eroding the existing U.S. technology of acquired companies; impacting the availability of upstream inputs; and undermining the ability of downstream purchasers and producers to compete.

Thus, CFIUS is under increased pressure to evaluate supply chain factors in its analysis and must also account for China's strategy of civil-military integration.[9]

III. The Recent Designations of ZTE, Huawei, and Other Chinese Technology Companies

On May 16, 2019, BIS added Huawei and 68 of its non-U.S. affiliates to the Entity List.[10] The U.S. Government did so after determining that there was reasonable cause to believe that Huawei had been involved in activities contrary to the national security or foreign policy interests of the United States. The specific activities contrary to the national security or foreign policy interests of the United States include those activities alleged in the Department of Justice's public superseding indictment of Huawei, including alleged violations of the International Emergency Economic Powers Act (IEEPA) and conspiracy to violate IEEPA (by providing prohibited financial services to Iran), and obstruction of justice in connection with the investigation of those alleged sanctions violations. As a result of its placement on the Entity List, the sale or transfer of American commodities, software, or technology to Huawei or its affiliates on the Entity List requires a license issued by BIS, and a license will

[9] See, "Washington unnerved by China's 'military-civil fusion,'" Kathrin Hille, Financial Times, November 8, 2019.

[10] 15 C.F.R. Pt. 744, Supp.4.

be presumptively denied. By publicly listing such persons, the Entity List is an important tool to protect U.S. national security and foreign policy interests.

Under the President's recent announcement, BIS will be promptly taking action to issue certain additional licenses, to companies that apply, which permit transactions that pose no national security risk, are not contrary to U.S. foreign policy interests, and are used to maintain, service and support: (A) widely available commodity chipsets and certain electronic integrated circuits; (B) software and tools that are generally available to the public; or (C) operating system software and applications and system services for mobile devices, as well as technology and software necessary to support the operating systems. Other license applications that pose no national security threat and are not contrary to U.S. foreign policy interests will also be promptly considered.

Prior to Huawei's designation, BIS also targeted ZTE. In March 2016, ZTE and several of its affiliates were added to the Entity List for their involvement in a scheme to reexport U.S.-controlled items to Iran. ZTE reached a settlement with BIS in March 2017, paying a total of US$1.19 billion in fines, and was subject to a suspended denial order. Having not complied with certain conditions of that settlement, BIS activated the Denial Order on ZTE in April 2018. The import ban has since been lifted as ZTE agreed to a settlement with BIS with significant conditions, including a US$1 billion fine. BIS rightfully took a strong stance against ZTE, imposing unprecedented compliance measures as part of the settlement. These actions demonstrate a robust commitment on the part of the Administration to combat technology-related national security issues. Such efforts were necessary and long overdue.

The effort to closely scrutinize and restrict transactions with Chinese entities that pose potential national security risks is not limited to the Administration. Congress, through Section 889 of the NDAA, has effectively banned the Federal Government from purchasing equipment from Huawei and ZTE, citing them as national security risks. Specifically, Section 889 prohibits Federal agencies, Federal contractors, and grant or loan recipients from procuring certain "covered telecommunications equipment or services," (equipment and services produced by Huawei and ZTE, and with respect to certain public safety or surveillance applications, Hytera Communications Corporation, Dahua Technology Company, and Hangzhou Hikvision Digital Technology Company) as a "substantial or essential component of any system, or as critical technology as part of any system." Congress clearly believes that taking a strong stance against national security threats is warranted and necessary. We have recently seen a concerted effort from Congress and the Administration to protect U.S. national security against threat actors in the technology and telecommunications sectors. Continued diligence in this area is crucial to protecting U.S. national security moving forward.

IV. Effectiveness of ECRA-Related Control Structures in the United States in Confronting the Challenges Raised with Respect to China, including Persistent Diversion Challenges

I believe that the ECRA-related controls will go a long way toward improving U.S. transparency and effectiveness in addressing the challenges related to China and its persistent diversion tactics. We have seen that stronger enforcement and broader application of law under FIRRMA has had an effect. As reported by a number of sources, including the Rhodium group, Chinese investments into the United States have been significantly curtailed. This was important given the statistics on Chinese government backed investment happening in our most advanced and innovative companies. The Rhodium group had calculated that, on average, 21 percent of Chinese venture investment in the United States from 2000 through 2017 came from state-owned funds, which are controlled at least in part by the Chinese government. In 2018, that figure surged to 41 percent.[11]

Also, with the implementation of ECRA and designation of emerging and foundational technologies, U.S. policymakers will be able to better assess the vulnerability of our supply chains and where the United States stands in terms of critical technology leadership, including where that leadership has been eroded.

However, clearly, we need a "whole of Government" defensive strategy where it concerns these national security threats. When China utilizes government actors to hack into U.S. private companies to take proprietary technology and give such information to Chinese companies, the United States must address the issue broadly. Pulling from a recent speech by the U.S. Justice Department, I note: "since 2011, more than 90 percent of the Department's economic espionage prosecutions (*i.e.,*

[11] See Reuters "Chinese tech investors flee Silicon Valley as Trump tightens scrutiny," by Heather Somerville, January 7, 2019.

cases alleging trade secret theft by or to benefit a foreign state) involve China, and more than two-thirds of all Federal trade secret theft cases during that period have had at least a geographical nexus to China. Some of those cases demonstrate that China is using its intelligence services and their tradecraft to target our private sector's intellectual property."[12] Clearly, we must continue to improve our ability to protect U.S. private companies from Chinese nation-state threat actors.

V. Possible Legislative or Oversight Recommendations

In closing, I applaud this Committee and this Administration for the hard work to create new and stronger mechanisms to address national security vulnerabilities arising from the loss of critical technologies, military, emerging and foundational. While implementation of ECRA and FIRRMA are underway, there is even more that could be done.

We should create additional enforcement tools to better address cyber and intellectual property ("IP") theft. Perhaps an IP "Entities List," similar to USTR's Notorious Markets List. Further we should consider taking additional actions in response to cyber attacks using executive powers. With the full implementation of FIRRMA, foreign government-controlled transactions and transactions involving critical infrastructure should be subject to mandatory filing requirements. We also need additional tools to address overcapacity by foreign state-owned enterprises that are able to enter the U.S. market unimpeded or create global market distortions to the detriment of our producers and U.S. innovation and jobs.

Last and importantly, the key to ensuring that BIS and other export control agencies are able to carry out their missions and the new responsibilities under ECRA is additional funding and resources. If we are serious about addressing the current and future loss of U.S. emerging and foundational technology, if we want to ensure that the United States continues to be a global leader for innovation, security and freedom, it is critical that such funding and resources is provided.

As Secretary Ross said: "We can no longer accept the decline of U.S. industries due to state-supported overcapacity, and the strategic—often clandestine—foreign purchases and investments in our most important technology enterprises."[13]

Thank you for the opportunity to appear before you today. I look forward to your questions.

PREPARED STATEMENT OF BEN BUCHANAN, PH.D.

ASSISTANT TEACHING PROFESSOR, SCHOOL OF FOREIGN SERVICE
SENIOR FACULTY FELLOW, CENTER FOR SECURITY AND EMERGING TECHNOLOGY
GEORGETOWN UNIVERSITY

JULY 18, 2019

Thank you, Chairman Crapo and Ranking Member Brown, for holding this important hearing and for inviting me to testify.

My name is Ben Buchanan. I am an Assistant Teaching Professor at the School of Foreign Service and a Senior Faculty Fellow at the Center for Security and Emerging Technology, both at Georgetown University. I am also a Global Fellow at the Woodrow Wilson International Center for Scholars, where I teach introductory classes on Artificial Intelligence and cybersecurity for congressional staff. My research specialty is examining how cybersecurity and AI shape international security. I co-authored a paper entitled "Machine Learning for Policymakers."[1]

As this Committee is well aware, export controls are legal tools that are applied to technology. If either the tool or the technology is not a good fit, export controls will fail. Given the expertise of my two fellow witnesses on the legal nuances of the tools themselves, I believe I will be of most value to the Committee in talking about some of the technologies in play and what makes export controls comparatively more or less suitable with these technologies. As a way of opening our discussion, I will focus on one particular suite of technologies that is particularly notable, artificial intelligence, but I believe this discussion will also apply to other relevant technologies.

---

[12] Remarks of Deputy Assistant Attorney General Adam S. Hickey of the National Security Division at the Fifth National Conference on CFIUS and Team Telecom, Washington, D.C., Wednesday, April 24, 2019.

[13] Remarks by U.S. Commerce Secretary Wilbur L. Ross at the Bureau of Industry and Security Annual Conference on Export Controls and Security, July 9, 2019.

[1] Buchanan, Ben and Taylor Miller. "Machine Learning for Policymakers." Belfer Center for Science and International Affairs (2017), *https://www.belfercenter.org/sites/default/files/files/publication/MachineLearningforPolicymakers.pdf.*

Conceptualizing AI

Nobody has a crystal ball, but there are other ways to consider our modern and near-future era of AI that will be useful for this discussion. To do so, it is important to understand how AI differs from so much of what came before it. An analogy will help.

One can imagine two ways of teaching a child to perform a task. The first is to give very clear instructions in a language the child understands about what the task is and how it is to be performed. The second is to show the child, through a series of examples, how the task works, and have the child infer the important rules and patterns necessary to get the job done. At various points in a child's education, they learn different tasks through each of these methods.

Traditional software development, and even some older versions of AI, work in a way that is similar to the first method. They rely on software developers understanding the problem to be solved in great depth, and then imparting this expertise to the system. For example, in a program designed to play chess, the software developers may consult with grandmasters to understand the optimal strategies for a wide range of situations, and then program those ideas into the code.

Modern AI systems, known as machine learning systems, use the second method, the one involving inference. In a machine learning system, rather than receive clear instructions about how to do the task, software developers create an algorithm that determines how the system should learn. They then provide that algorithm with lots of relevant data and computational power (the processing hardware that makes machine learning algorithms function).

There are thus three parts to this system: the algorithm, the data, and the computational power. Together, they form an essential triad. Each is more or less important in various versions of machine learning, but at the same time, each in its own way is critical. To understand why, it is worth examining the triad in a little more detail.

Data

It is in vogue to say that data is the new oil. This is because, to use the second kind of program I described above—the machine learning method—a lot of relevant data is often required. From this data the machine learning system will infer important patterns and nuances, and will determine what success and failure look like. It is thus vital that the data provided to the machine be representative of the problem in all its complexity and plentiful.

A large part of the reason that companies like Google, Amazon, and Facebook are successful with the AI systems they deploy is because they aggregate gigantic amounts of data. In essence, the large datasets these companies assemble provide them with a competitive advantage over others. Large companies based in other nations, such as China's Baidu, Alibaba, and Tencent, derive similar advantages from their datasets. It seems to me that export controls are unlikely to be of much use in managing this competition or guarding against potential threats from data, both because companies already have an incentive and tools to secure and not share their assembled data and because export controls are comparatively ill-equipped to stop the transfer of sensitive data relative to other tools like classification (for government data), and licensing or contractual restrictions regardless of export.

Algorithms

Algorithms are the second component of the AI triad. These software instructions dictate how the machine learning system will learn. They stipulate how it will interpret the data, what sort of capabilities it will develop, and what inferences it will learn to draw that can be applied to future tasks. There are a wide variety of algorithms, each suited to different kinds of tasks, from classifying images to making predictions about housing prices based on historical trends, to generating new pictures of people who look real but do not actually exist. The algorithmic frontier is rich, and a great deal of progress has been made in the last 7 years.

The prevailing ethos is that, once an algorithmic advance is made, researchers post it online and share it with others. In this sense, AI research is remarkably open, far more so than the fierce competition of the technology industry would normally suggest. There are exceptions to this practice, instances in which algorithms have not been published due to national security concerns—most notably a decision by OpenAI, a leading research lab, not to publish a powerful algorithm that could be used to generate realistic-fake text.

That said, the experience of several decades has shown that government efforts to control the export of computer code are usually futile, and I think it is fair to say that export controls are unlikely to be useful in stopping all but the most powerful of algorithms. And even with those most powerful algorithms, I have doubts

about the suitability of our current list-based export control systems, given the changing pace of technology and the movement of the technological frontier.

Computing Power

This brings us to the last part of the triad: computing power, or what AI researchers simply call "compute." It is easy to ignore, but it remains vitally important, perhaps prohibitively so. In the last 7 years, we have witnessed a revolution in computing power applied to machine learning. One study by OpenAI indicated that between 2012 and 2018, the computing power applied to top machine learning systems increased by a factor of 300,000; if a cell phone battery lasted 1 day in 2012 and increased by the same factor, that battery would now last 800 years.[2]

There is much to discuss about why this increase in computing power has occurred, but the most salient factor for our purposes today is that, unlike algorithms and data, computing power is a function of hardware, not software. That is, computers are tangible products that are easier to manage, including with export controls. My judgment is that, to the degree that export controls are relevant to the problem of managing AI and other technologies such as 5G, it will controls on this hardware component, and likely on the hardware that manufactures specialized computer chips for AI. This statement is both a commentary on the limitations of export controls to the problem but also on the more narrow areas where they might be suitable for protecting national security.

To be clear, in order for any such controls to work—whether on AI hardware or something else—they must be conducted in a multilateral fashion with allies, given that a great deal of hardware engineering expertise is outside the United States.

I thank you again for holding this hearing and the opportunity to lay out the basics of this complicated, fast-changing field for your consideration as you review the implications of export control for AI and other technologies. As you know, it is vital that we both protect national security and not squash innovation. This is an area that the Center for Security and Emerging Technology has been studying, and we expect to publish our analysis on it in the weeks to come. In the meantime, I look forward to your questions.

[2] "AI and Compute," OpenAI, (2018), *https://openai.com/blog/ai-and-compute/*.

RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN CRAPO FROM ERIC L. HIRSCHHORN

Q.1. *Expansion of Scope*—Traditionally our export control system has focused on national security and foreign policy.

Should we expand the focus of our controls to address issues of economic competitiveness like Made in China 2025?

A.1. No one can deny the serious policy implications for the United States of the Made in China 2025 plan. Artificial state subsidies of particular technology sectors are market distorting and put U.S. companies at a competitive disadvantage. ECRA correctly recognizes, though, that in today's interdependent world, multilateral controls are far likely than unilateral controls to be successful.[1] For that reason, expanding U.S. controls to address issues of economic competitiveness, though tempting, might be self-defeating. We generally have been successful in recent decades in convincing our allies to join us in controlling exports of items that could put our collective national security at risk or engender the spread to undesirable end users of weapons of mass destruction. This has been so despite our allies' often-expressed suspicions—and our truthful denials—that the U.S. is seeking economic as well as national security advantage. To expand our export controls to expressly address economic competitiveness concerns could lead our allies to think twice about supporting our efforts.

Some observers contend that if the U.S. were to take the lead in imposing controls on technology exports of technology to China for economic reasons, our allies would follow the example. I doubt it. Our allies have traditional views of export controls and probably would not agree to control the flow of technology for other than the traditional national security and foreign policy objectives that are set out in ECRA.

Q.2. *Foundational Technologies*—Are there any "foundational" technologies that are not, by definition, already widely available?

A.2. Neither ECRA nor FIRRMA nor—so far, at least—the Administration has defined the term "foundational." I have assumed that it refers to technologies that are widely available—*i.e.,* technologies that are export controlled, if at all, only to the handful of countries that are designated as supporting terrorism. I have been told that the executive branch shares that view of what the term means. Unilaterally controlling technologies that are widely available from other countries would harm our domestic economy without preventing China and other countries of concern from acquiring such technologies. The Administration's task, then, is to ascertain whether there are "foundational" technologies that (1) are useful to China and (2) "essential to the national security of the United States"[2] but (3) not widely available elsewhere, and then—as required by ECRA[3]—seek multilateral control of such technologies.

Q.3. *Evidence of Controls Driving Offshore Activity*—Is there any evidence that tight export controls drive research and development, or manufacturing, offshore?

---

[1] ECRA §1752(4)–(6) (codified at 50 U.S.C. §4811(4)–(6)).
[2] ECRA §1758(a)(1)(A) (codified at 50 U.S.C. §4817(a)(1)(A).
[3] ECRA §1758(c) (codified at 50 U.S.C. §4817(c)).

A.3. In recent decades we have seen this phenomenon in the areas of machine tools, commercial space items, and thermal imaging items. All were subject to very tight U.S. export controls. The development and manufacturing competition that grew up abroad in each of those sectors was, I believe, largely a result of that action on our part. As long ago as the 1990s, I had clients tell me that they were shifting their R&D offshore because of the extreme tightness of U.S. export controls on their types of technology. Our country narrowly avoided this fate in two other sectors, namely encryption and computers, because we relaxed our controls somewhat once we realized that the horse already was out of the barn.

In a world where advanced technologies can be developed and produced in many countries, the logic of unilateral controls versus multilateral controls is clear. If a company cannot legally export a technology from one country, it will likely seek to develop and that technology in a country that does not prohibit such exports. Moreover, investors will make their investments in such countries rather than in the United States. Unilateral controls thus can harm the U.S. industrial base and enhance the industrial base of foreign competitors without preventing the proliferation of the technology to countries of concern. For this very basic, logical, economics-driven reason, Congress wisely provided in ECRA that unilateral controls are disfavored.

Q.4. *Control Rulings*—ECRA essentially requires an interagency review of decisions to add or remove items from the control lists and to approve or deny individual license applications.

Is Commerce the best department to lead the dual-use export control system?

What would be the harm if we transferred the export control system to the Defense Department for it to decide what should or should not be exported?

A.4. Commerce has administered controls on dual-use items since the late 1940s, with lower-level military items being added in recent years as part of the Export Control reform initiative. For about 25 years, the Defense, State, and Energy departments have been empowered to review any Commerce license application—and in fact do review almost all such applications. Moreover, any changes to the regulations, including additions to and subtractions from the control lists, essentially require consensus of the four agencies before they may be implemented. Contrary to the false statements of some that Commerce somehow routinely "overrules" Defense on national security judgments and State on foreign policy judgments, the current system does an excellent job of accounting for the expertise and equities of different parts of the Government. To quote a sage Washington observer from the past—"If it ain't broke, don't fix it."

Moreover, such controls long have taken into account not only potential military applications, as to which the Defense Department has special expertise, but also such salient issues as foreign availability, foreign policy, and the like, where Commerce and State bring their expertise to the table. ECRA has it right: Commerce controls should take into account their "impact on the economy of the United States" and should be imposed "only to the extent nec-

essary" to achieve U.S. national security and foreign policy aims.[4] The considerations set out in ECRA include the strength of the U.S. defense industrial base—a role shared by Commerce and Defense under the Defense Production Act of 1950—the maintenance of U.S. leadership in the "science, technology, engineering, and manufacturing sectors," and foreign availability.[5] Defense already—and appropriately—has a full voice when it comes to potential military application of technology but the voices of Commerce, State, and, where nuclear issues are concerned, Energy also are essential to the proper functioning of the system. Commerce has technical and policy expertise in all these areas but has demonstrated particular skill in administering and enforcing a reliable, predictable regulatory regime that pursues all these objectives.

Q.5. *Huawei Delisting*—The addition of the Huawei to the Commerce Department's Entity List is one of the most public and significant export control topics in today's headlines.

Without commenting on Huawei, could you tell us what the Entity List is, its purpose, and whether or not it has been historically effective and how is it different from a civil or a criminal penalty, a denial order, a Treasury Department sanction, or other actions the U.S. Government can take against a foreign company?

A.5. In a strictly legal sense, the Entity List is fairly low on the totem pole of actions the United States can take against a company. It imposes no criminal, civil, or administrative penalty against a named party but merely requires that all items "subject to the Export Administration Regulations" require a license to be exported to that party. Of course, this means that many items that don't need a license to go to anyone else will have to wait while a license application is submitted, considered, and possibly denied. Importantly, items that are not "subject to the EAR" are not caught by a foreign importer's appearance on the Entity List. That means that unlike, say, sanctions administered by the Treasury Department's Office of Foreign Assets Control, the Entity List doesn't reach foreign-made items located outside the U.S., even if they're sold from such locations to Entity List companies by U.S. companies.

The most common reason for placing a company on the Entity List is to encourage it to clean up its act in terms of respecting U.S. export controls. Once it has demonstrated its compliance, and provided relevant information to the Office of Export Enforcement at Commerce, the company can seek removal from the List. Absent the possibility of removal in exchange for cooperation, there is little incentive for a listed company to cooperate with the U.S. Government.

As difficult as the formal effect of being on the Entity List may make a company's life, the secondary and unofficial effect can be worse. This is because financial institutions and large companies throughout the developed world use software to screen for "bad" customers. That software includes everyone who's been fined, indicted, listed as a denied party, debarred, or placed on the Entity List. So although the Entity List technically isn't a penalty, compa-

[4] ECRA §1752(1) (codified at 50 U.S.C. §4811(1)).
[5] ECRA §1752(2)(C), (3), (6) (codified at 50 U.S.C. §4811(2)(C), (3), (6)).

nies listed there get added to that software, too. That in turn means that many such financial institutions and companies simply will refuse to do business with them.

The only less draconian action than the Entity List is the Unverified List. Placement there usually means that U.S. officials have not been permitted to make post-shipment visits to the entity in question to check whether the U.S.-origin items supposedly sent there actually are there. Often the reason is that the host government, rather than the consignee company, is the problem. Exporters may ship to parties on the Unverified List without obtaining additional licenses but they are on notice that such parties' bona fides are uncertain and that accordingly they should take care to satisfy themselves that the orders are legitimate.

Q.6. The United States has a special treatment arrangement with Hong Kong with regards to export controls. While it is in the United States interests to have a strong economic relationship with Hong Kong, there is a lot of concern about growing Chinese encroachment on Hong Kong's autonomy and the potential implications for safeguarding technology.

Is our current export control policy equipped to deal with risk of diversion from Hong Kong to China?

What are some ways in which China is using or could use Hong Kong as a vector for acquisition of technology that we do not export to the Mainland?

What are your specific recommendations for strengthening our export control regime in relation to these challenges?

A.6. The concerns expressed in these questions are legitimate and not new, though recent efforts of the Chinese government to narrow Hong Kong's autonomous status of course bring them to the fore. In my experience, cooperation between the United States and Hong Kong customs and export control authorities has been good but Hong Kong is a very busy place with close political and commercial ties to China. The Obama administration strengthened protections against unauthorized diversions to China via Hong Kong by requiring "persons intending to export or reexport to Hong Kong any item subject to the Export Administration Regulations (EAR) and controlled on the Commerce Control List (CCL) for national security (NS), missile technology (MT), nuclear nonproliferation (NP column 1), or chemical and biological weapons (CB) reasons to obtain, prior to such export or reexport, a copy of a Hong Kong import license or a written statement from the Hong Kong government that such a license is not required."

That rule "also requires persons intending to reexport from Hong Kong any item subject to the EAR and controlled for NS, MT, NP column 1, or CB reasons to obtain a Hong Kong export license or a statement from the Hong Kong government that such a license is not required."[6]

I don't know enough about our experience under the 2017 rule to have a view on whether it is working well. I would encourage continued vigilance over reexports of U.S.-origin items from Hong Kong, including compliance with that regulation. Such vigilance is possible, though only if BIS has the resources to carry it out.

[6] 82 FR 6216 (Jan. 19, 2017).

Congress should appropriate additional funds to BIS so that it can do this work, as well as its other work, thoroughly and effectively.

RESPONSE TO WRITTEN QUESTION OF SENATOR BROWN FROM ERIC L. HIRSCHHORN

Q.1. The press have reported widely on China's surveillance state and their gross human rights violations of the Uyghur people. Whether the technology is organically developed or stolen IP from American companies, we should all be concerned with how technology can be perverted to violate civil liberties and basic human rights.

Mr. Hirschhorn, walk me through how the interagency takes issues like human rights violations into consideration when discussing emerging technologies. What are the mechanisms to mitigate the unintended consequences of bad actors or countries misusing these technologies, and can that process be improved?

A.1. ECRA sensibly requires that the consideration of export control policies, as well as individual licensing decisions, take human rights into account.[1] This applies not only to emerging technologies but all export control policies and license reviews. Applications for Commerce Department export licenses are shared with the Department of State, whose Bureau of Democracy, Human Rights, and Labor (DRL) is among the bureaus consulted internally at that department. The State Department has an equal vote with Commerce, Defense, and Energy at all levels of the process for reviewing applications for Commerce export licenses. Moreover, human rights are not the exclusive province of State. Commerce, Defense, and Energy can and do raise human rights concerns about BIS license applications.

Part of the difficulty in ensuring protection of human rights is that sometimes the technologies employed to violate human rights are controlled to only a handful of countries because they are fairly basic or general purpose, they're widely available from sources other than the United States, or both. Where that is the case, refusal to allow the export of U.S. products may make an appropriate statement from a foreign policy standpoint but have little or no practical effect on the target government.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARREN FROM ERIC L. HIRSCHHORN

Q.1. At least one U.S. company has been found to have provided the Chinese government with a tool enabling it to monitor Uyghur and Central Asian minorities, as part of what one Uyghur activist described in April 9, 2019, testimony to the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy as "an Orwellian mass surveillance state" where "more than one million Uyghurs are arbitrarily detained outside the legal system in concentration camps." A bipartisan group of Senators introduced the Uyghur Human Rights Policy Act, of which I am a cosponsor, which states in part, that:

---

[1] ECRA §1752(2)(D) (codified at 50 U.S.C. §4811(2)(D)).

> the Secretary of Commerce should review and consider prohibiting the sale or provision of any United States-made goods or services to any state agent in Xinjiang, and adding the Xinjiang branch of the Chinese Communist Party, the Xinjiang Public Security Bureau, and the Xinjiang Office of the United Front Work Department, or any entity acting on their behalf to facilitate the mass internment or forced labor of Turkic Muslims, to the "Entity List" administered by the Department of Commerce.

Please explain your view. Do you agree?

A.1. The United States has imposed end-user-specific restrictions such as this on many occasions. Indeed, ECRA's provision that U.S. export controls should "carry out the foreign policy of the United States, including the protection of human rights and the promotion of democracy"[1] provides ample legislative authority for such an action.

Q.2. Can you conceive of any circumstances under which it would be appropriate for the United States to weaken our export control laws and regulations, or the enforcement of those laws and regulations, *vis-a-vis* China or any other foreign competitor in order to extract concessions or other commitments from that foreign competitor on matters related to trade or human rights? Please explain your view.

A.2. I'm not prepared to say that such circumstances never could arise but it would have to be an extraordinary case. The recent suggestions by the President that extensive export control violations by a Chinese telecommunications company should be traded for sales of beef, chicken, soybeans, and the like do not meet that criterion, and seriously undermine our military and our law enforcement.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM ERIC L. HIRSCHHORN

Q.1. You said in your testimony you believed for export controls to be effective, they should be adopted both by our allies and unilaterally imposed by us.

What are the challenges you foresee in convincing allies to align with us on this issue and how can we overcome them?

A.1. When it comes to issues of military security and preventing the spread of weapons of mass destruction, we have had great success over the past 70 years in convincing our allies to go along with controls that are proposed by the United States. In the area of foreign policy, most notably with regard to Cuba, we have had relatively support from our allies. The greatest obstacles to convincing allies to cooperate are closely related to one another. First is their oft-expressed view—one that is incorrect—that we somehow use such controls to further our own economic and commercial interests. Second is the fear that U.S. exporters don't share equally in the harm that necessarily flows to domestic parties from any country's export controls and economic embargoes.

---

[1] ECRA §1752(2)(D) (codified at 50 U.S.C. §4811(2)(D)).

The best way to convince our allies to cooperate is to continue—as ECRA prescribes [1]—to limit our export controls to those driven by military, intelligence, and foreign policy considerations.

Q.2. You said in your testimony it is hard to draw up export controls for certain emerging technologies because you run the risk of being too generic or broad, which would make the controls difficult to enforce.

What is the best way to address this problem to ensure regulations are as specific to technology and application as possible?

A.2. The best way to ensure the requisite specificity is pretty much to continue doing what the executive branch has been doing for decades, namely keeping a close eye on emerging technologies but not imposing controls until it's clear what uses the technologies are being put to and which of those uses have demonstrable potential for military or intelligence use by adversaries.

ECRA sensibly provides that, in deciding whether to identify a technology that's "essential to the national security"[2] as being "emerging" or "foundational," and impose unilateral controls on its export, the Administration take into account—

- the development of the technologies in foreign countries;
- the effect that such export controls may have on the development of such technologies in the United States; and
- the effectiveness of export controls imposed pursuant to this section on limiting the proliferation of emerging or foundational technologies to foreign countries.[3]

Moreover—and this was a valuable lesson of the Export Control Reform initiative—an important way to limit the possibility that the Government mistakenly will under or over-control emerging technologies (or any technologies, for that matter) is to seek public comment on proposed controls before actually implementing them. ECRA wisely requires this.[4]

Q.3. To what extent does the Commerce Department collaborate with developers to understand what technological aspects should be controlled under ECRA?

A.3. I have been out of the Government for nearly three years and don't know what contacts those administering our export controls currently have with the private sector. During my tenure, we found the input from BIS' technical advisory committees, as well as from general requests for public comment, to be of great value in ensuring that our controls would be appropriate. BIS would be wise to continue and expand this policy.

Q.4. I am also concerned that if we too tightly regulate the export of some technologies, we will drive our innovation and production offshore, as you suggested in your testimony.

In your experience, what is the best way to ensure that we are maintaining our global leadership in technology, while also not contributing to adversarial countries' best efforts to surpass us?

---

[1] ECRA §1752(1), (11) (codified at 50 U.S.C. §4811(1), (11)).
[2] ECRA §175(a)(1)(A) (codified at 50 U.S.C. §4817(a)(1)(A)).
[3] ECRA §1758(a)(2)(B) (codified at 50 U.S.C. §4817(a)(2)(B)).
[4] ECRA §1758(a)(2)(C) (codified at 50 U.S.C. §4817(a)(2)(C)).

A.4. In recent decades we have seen this phenomenon in the areas of machine tools, commercial space items, and thermal imaging items. All were subject to very tight U.S. export controls. The development and manufacturing competition that grew up abroad in each of those sectors was, I believe, largely a result of that action on our part. As long ago as the 1990s, I had clients tell me that they were shifting their R&D offshore because of the extreme tightness of U.S. export controls on their types of technology. Our country narrowly avoided this fate in two other sectors, namely encryption and computers, because we relaxed our controls somewhat once we realized that the horse already was out of the barn.

The message here is that these are judgment calls and that more is not always better. Although potentially dangerous technologies of course should be controlled, overly tight controls—especially if they are unilateral—can be as damaging as overly loose controls. The result in the thermal imaging area, for example, has been that we have significant foreign competition and—even more important from a security standpoint—have no window into, or influence regarding—where those foreign products end up. Had we been a shade more reasonable in deciding how tightly we should control that technology, other countries might have had less of an incentive to create their own thermal imaging manufacturing capability.

Sixteen years ago I presented a paper on this point, "Export Issues for Military Sensors: The Fork in the Road," at a Military Sensors Symposium sponsored by the U.S. Army's Night Vision and Electronic Sensors Directorate.[5] The symposium was attended by many of our Government's leaders in the thermal imaging field. My conclusion, which regrettably was prophetic, was as follows:

> The United States long has been the unchallenged leader in sensor technology but a move offshore of production—and leadership—is imminent. Commercial demand for American sensor products is burgeoning but the bottleneck caused by export restrictions has created a supply shortage abroad. Foreign technology and products are rushing to fill this foreign demand. They may not yet have matched United States technological standards but they will get there quickly, especially if we continue, in effect, to cede foreign markets to foreign suppliers. Reasons of national security . . . make it crucial that this not occur. There is no doubt that it will occur, however, if the current overcontrol of sensors is not adjusted to comport with reality.

Subsequently, we saw the development of robust thermal imaging industries in France, Israel, and China, among others. We now have little or no visibility of, and little or no influence about, where the products of those countries—particularly those that are not members of the Wassenaar Arrangement—end up. This might have been different had we been more nuanced about how we controlled this technology.

---

[5] Eric L. Hirschhorn, "Export Issues for Military Sensors: The Fork in the Road," presented at Military Sensors Symposium sponsored by Night Vision and Electronic Sensors Directorate, Department of the Army (Oct. 2003) (proceedings classified Secret; this paper Unclassified and approved for unlimited public release).

RESPONSE TO WRITTEN QUESTION OF SENATOR SINEMA FROM ERIC L. HIRSCHHORN

Q.1. There appears to be consensus that a multilateral approach to export controls is most effective in mitigating technologies that threaten U.S. industry and national security. It also appears there is consensus that multilateral efforts will work best in restricting divisive Chinese technology and infrastructure. Given the importance of a multilateral approach and the serious national security threats China poses, are you at all concerned that the Administration's policies and rhetoric on trade could undermine the necessary goodwill to work collaboratively with our trading partners to hold China accountable?

A.1. I am of two minds about this issue. Sovereign nations generally are more able to look out for and pursue their own best interests than, say, individuals within our country. That means that if they see an advantage in cooperating with the United States on export controls and economic sanctions, they will do so despite the rude treatment that they may have been receiving from the current administration. That said, not every aspect of international relations is bloodless and devoid of personal emotion. There quite possibly will be cases where our poor treatment of an ally will discourage it from cooperating with us.

RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN CRAPO FROM NOVA J. DALY

Q.1. *Expansion of Scope*—Traditionally our export control system has focused on national security and foreign policy.

Should we expand the focus of our controls to address issues of economic competitiveness like Made in China 2025?

A.1. Chairman Crapo, thank you again for the opportunity to testify before the Senate Committee on Banking, Housing, and Urban Affairs. It was an honor. The following responses to questions are based on my own views and do not reflect those of my firm, Wiley Rein LLP, nor any client.

Under the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which governs the Committee on Foreign Investment in the United States (CFIUS), Congress included as a national security consideration acquisitions of critical technology as they affect U.S. leadership in areas related to national security. Such considerations were also included in the precursor legislation to FIRRMA, the "Foreign Investment and National Security Act of 2007." Further, one of the factors included in the first CFIUS bill is "the potential effects of the proposed or pending transaction on United States international technological leadership in areas affecting United States national security." Thus, there is clear precedent for treating critical technology protection and leadership as a core national security consideration. Adding to this precedent, in December 2017, the Trump administration published its "National Security Strategy of the United States of America." That document states that "economic security is national security."

As may you know, and as reflected in my testimony, China's "Made in China 2025" initiative emphasizes China's priorities for high-tech industries. The Chinese strategy lists multiple tech-

nologies where it seeks global dominance. These technologies include those that are or may be subject to U.S. export controls and therefore raise national security and foreign policy considerations. Placing appropriate controls on emerging and foundational technologies should be undertaken in a targeted way to address those Made in China 2025 initiatives that raise national security and foreign policy considerations.

Such undertakings are already underway. The Department of Commerce's 14 proposed emerging technology categories mirror in some respects the industries China identified as part of its Made in China 2025 initiative. Congress itself could also consider the national and economic security effects of China's "military-civil fusion," which has been a strategic initiative for some time. The goal of this initiative is the assimilation of China's technology industry into its defense industry in order to propel the advancement of dual-use technologies.

I applaud the U.S.-China Economic and Security Review Commission for holding a hearing earlier this year on the topic of "Technology, Trade, and Military-Civil Fusion," thus raising this issue with Congress. I believe that it is imperative that we expand the focus of our export controls to address Made in China 2025 issues that raise national security and foreign policy considerations.

Q.2. *Foundational Technologies*—Are there any "foundational" technologies that are not, by definition, already widely available?

A.2. The Bureau of Industry and Security (BIS) announced that an advance notice of proposed rulemaking (ANPRM) would be issued seeking public comment on criteria for identifying "foundational" technologies. However, the ANPRM has not yet been issued. Without this list, it is difficult to answer this question comprehensively. That said, when the list is issued, it will be important to address "point of the spear" technologies within each category of foundational technologies. For example, semiconductors are likely to be considered a foundational technology. Within semiconductors, the Administration could consider targeting technologies involving gallium nitride (GaN) for any additional export control authorities.

Q.3. *Evidence of Controls Driving Offshore Activity*—Is there any evidence that tight export controls drive research and development, or manufacturing, offshore?

A.3. I am aware of anecdotal evidence that tight export controls have caused lost sales that led to increased sales and manufacturing by foreign competitors. This is a historic consequence of having export controls for every country that has them. However, to address this issue, we must always seek to ensure that we apply export controls appropriately, while taking account of commercial considerations. The United States should continue to work with its multilateral partners to ensure a broader consensus and consistent application of export controls. However, unilateral export controls may be required where we know an adversary is or could utilize such technology for military or nefarious purposes.

Q.4. *Control Rulings*—ECRA essentially requires an interagency review of decisions to add or remove items from the control lists and to approve or deny individual license applications.

Is Commerce the best department to lead the dual-use export control system?

A.4. The Department of Commerce is the right agency to lead the dual-use export control system because of its breadth of experience and history of authority in this area. Commerce has authority and expertise beyond BIS, including under the International Trade Administration (ITA) and various bureaus that focus on different sectors of the U.S. economy. BIS is therefore able to collaborate with other bureaus, including within ITA, to build expertise on global economic matters and commercial considerations where export control policies requires broader considerations.

Q.5. What would be the harm if we transferred the export control system to the Defense Department for it to decide what should or should not be exported?

A.5. While the U.S. Department of Defense (DOD) has significant resources, it currently does not have the depth of historical knowledge or sector-specific resources that the Department of Commerce has in the application of all dual-use technologies. While DOD has expertise and experience on certain core military technologies, Commerce has a breadth of economic resources and industry knowledge important to the assessment and application of export controls to dual-use technologies.

Q.6. *Unfair Trade Practices*—China engages in unfair trade practices and artificially subsidizes its companies in order to over-develop and over-produce in key sectors, such as semiconductors, in order to dominate the world marketplace. In order to protect the economic viability of U.S. companies, some propose we use export control rules to cut off the flow of basic commercial technology that the Chinese need to compete against U.S. companies—even if the technology has nothing to do with national security or foreign policy objectives.

If we take this approach, what's to prevent a non-U.S. company, such as in Europe or Japan, from simply filling behind or "designing out" the U.S. company and profiting off U.S.-only prohibitions being applicable only to U.S. companies?

A.6. Under the Export Control Reform Act of 2018 (ECRA), Congress stated that it is the policy of the United States "[t]o use export controls only after full consideration of the impact on the economy of the United States and only to the extent necessary" to restrict exports (1) that would make a significant contribution to the military potential of any other country that would prove detrimental to U.S. national security or (2) if necessary to significantly further U.S. foreign policy interests or to fulfill international obligations. (Sec. 1752).

Engagement with our multilateral partners is key to preventing such outcomes. Export controls, where harmonized, are much more effective. Toward that end, I understand that BIS is actively engaging with like-minded partners to discuss coordinating policies on emerging technologies. The U.S. should fully pursue engagement with multilateral partners to come up with combined agreement on

what should or should not be exported and also to improve information-sharing between allies.

Q.7. *Unilateral Controls*—Under what circumstances should the United States impose a unilateral control—that is, a control that only the United States imposes—on the export to China of a U.S.-origin commodity or technology?

A.7. Where there are clear economic security and national security concerns, especially where there is a choke point in the application of controls, or where our allies are unwilling to move to create multilateral controls, the United States has a responsibility to do so for its own national security interests. The U.S. should responsibly implement unilateral controls where clear economic security and national security interests arise.

Q.8. If there is such a case, what would prevent either a U.S.-subsidiary or non-U.S. company from simply selling such items outside the United States, thus enhancing the foreign company and harming the U.S. company?

A.8. Addressing export controls, especially those concerning emerging and foundational technologies, requires engagement with U.S. companies large and small, Congressional resources and oversight, and effective compliance regimes at the company level. Thus, U.S. companies, including their subsidiaries, must be aware that certain potential "business" partners or activity actually represent the interests of adversarial foreign governments who will use such technology and know-how to the economic security and/or military detriment of the United States.

There has always been a problem arising from the application of export controls when foreign countries and companies sell items controlled by U.S. export laws and regulations to the detriment of U.S. companies. That is why it is critical to build broad coalitions with our allies on export controls and, where we apply them unilaterally, to do so appropriately and with a clear understanding of economic considerations.

Q.9. The United States has a special treatment arrangement with Hong Kong with regards to export controls. While it is in the United States interests to have a strong economic relationship with Hong Kong, there is a lot of concern about growing Chinese encroachment on Hong Kong's autonomy and the potential implications for safeguarding technology.

Is our current export control policy equipped to deal with risk of diversification from Hong Kong to China?

A.9. No export control system is foolproof, but BIS has sought to address the risk of diversion from Hong Kong to mainland China, including with rules that went into effect in April 2017. In particular, these rules impose new requirements and supporting documentation for exports of specific controlled items to Hong Kong and build teams that do end-use checks. BIS has also issued guidance on due diligence factors for exporters to consider in order to prevent unauthorized transshipment or reexport of controlled items through Hong Kong to China.[1]

[1] U.S. Department of Commerce Bureau of Industry and Security, "Guidance on Due Diligence to Prevent Unauthorized Transshipment/Reexport of Controlled Items through Hong Kong to

Q.10. What are some ways in which China is using or could use Hong Kong as a vector for acquisition of technology that we do not export to the Mainland?

A.10. While I do not have direct expertise on this matter, it is not difficult to imagine that Chinese entities currently do and would use companies in Hong Kong to gain access to U.S. controlled technologies. They would likely do so through Hong Kong companies aligned with or having close commercial ties to mainland companies and/or customers.

Q.11. What are your specific recommendations for strengthening our export control regime in relation to these challenges?

A.11. I would suggest additional funding for BIS and additional oversight by Congress. For BIS, funding could be provided for more end-use checks to be conducted per annum based on past performance, and BIS could use help on targeting end-use checks in Hong Kong through upfront research on no license required shipments prior to post shipment verification requests, enhanced and continued intelligence sharing within BIS, and the utilization of intelligence information to help identify appropriate end-use checks.[2] The continued attention of Congress to such matters is paramount to successful U.S. efforts to counter reexport of export-controlled goods from Hong Kong to China.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR BROWN FROM NOVA J. DALY

Q.1. Mr. Daly, I want to hear your views on whether we should be developing additional tools to combat the Chinese government's efforts to dominate specific sectors.

Just as with developing emerging technologies, the Chinese government is strategic about the amount and targets of Chinese investment abroad. We've seen the results of that strategy in the U.S. rail car manufacturing sector, and there are recent reports about Chinese state-owned-enterprises investing in our energy sector.

Senator Grassley and I have a bill, the Foreign Investment Review Act, which would authorize the Secretary of Commerce to review foreign investments—particularly those made by Chinese state-owned enterprises—to make sure they're in our long-term economic interests.

Do you agree that there is value in establishing an investment screen in place to combat China's threats to our economic security?

A.1. I greatly appreciate the purpose of the Foreign Investment Review Act (FIRA) and Senator Brown and Senator Grassley for continuing to raise the issue of addressing Chinese efforts to make certain detrimental targeted investments in the United States and through state-owned enterprises. Understanding the effects of certain transactions on U.S. economic and technology leadership, especially those emanating from China or those with a nexus to China,

---

China," 2016, *https://www.bis.doc.gov/index.php/policy-guidance/hong-kong-due-diligence-guidance.*

[2] *Id.* at 27.

is very important, and such transactions should be appropriately reviewed.

As you may know, currently, CFIUS legislation, as modified by FIRRMA, is undergoing a regulatory process of implementation. FIRRMA establishes processes that require mandatory filing of certain technology transactions and certain transactions involving foreign government ownership. The CFIUS "Pilot Program" which addresses technology acquisitions, is well underway, and it will be useful to see how that program has helped to address threats to our critical technology leadership, an important element of our national and economic security. The mandatory filing requirement for transactions involving government-controlled entities could have been based on a control standard, as found in FIRA, rather than on ownership levels. Doing so would have likely increased filings made to CFIUS. It may be useful to consider legislation that would more narrowly apply the control standard to certain investments made by state-owned or controlled entities emanating from certain foreign investors from certain foreign countries. Nonetheless, the FIRA bill is helpful legislation and should have further congressional consideration.

Q.2. The press have reported widely on China's surveillance state and their gross human rights violations of the Uyghur people. Whether the technology is organically developed or stolen IP from American companies, we should all be concerned with how technology can be perverted to violate civil liberties and basic human rights.

Please discuss how the interagency process takes issues like human rights violations into consideration when discussing emerging technologies. What are the mechanisms to mitigate the unintended consequences of bad actors or countries misusing these technologies, and can that process be improved?

A.2. The protection of human rights is specifically mentioned in the Statement of Policy in the Export Controls Act of 2018.[3] Export controls are currently in effect for crime control categories.[4] The Department of State submits country Reports on Human Rights Practices to Congress, which is used by State and the Department of Commerce to deny licenses for export of crime control items to any country whose government engages in a consistent pattern of violations of internationally recognized human rights in accordance with the Foreign Assistance Act. Further, State is developing guidance for exporters of items with intended and unintended surveillance capabilities. The guidance seeks to provide insight to exporters on considerations to weigh prior to exporting these items. It also offers businesses greater understanding of the human rights concerns the U.S. Government may have with the export. Lastly, recently, using the interagency process, BIS added the Xinjiang Uyghur Autonomous Region People's Government Public Security

[3] National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115–232 (H.R. 5515) sec. 1752, 115th Cong, (2018).

[4] Department of Commerce Bureau of Industry and Security, "2018 Report on Foreign Policy-Based Export Controls," *https://www.bis.doc.gov/index.php/documents/pdfs/2186-bis-foreign-policy-report-2018/file.*

Bureau, 18 of its subordinate municipal and county public security bureaus, and another subordinate institute to the Entity List.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARREN FROM NOVA J. DALY

Q.1. At least one U.S. company has been found to have provided the Chinese government with a tool enabling it to monitor Uyghur and central Asian minorities, as part of what one Uyghur activist described in April 9, 2019, testimony to the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy as "an Orwellian mass surveillance state" where "more than one million Uyghurs are arbitrarily detained outside the legal system in concentration camps." A bipartisan group of Senators introduced the Uyghur Human Rights Policy Act, of which I am a cosponsor, which states in part, that:

> the Secretary of commerce should review and consider prohibiting the sale or provision of any United States-made goods or services to any state agent in Xinjiang, and adding the Xinjiang branch of the Chinese Communist party, the Xinjiang Public Security Bureau, and the Xinjiang Office of the United Front Work Department, or any entity acting on their behalf to facilitate the mass internment or forced labor of Turkic Muslims, to the "Entity List" administered by the Department of Commerce.

Do you agree? Please explain your view.

A.1. The continued promotion of human rights and religious freedom is an important matter in the consideration of export control policy. I applaud the continued efforts of the Members of the Committee on Banking, Housing, and Urban Affairs to promote religious freedom and human rights in China and around the world and the purpose of the Uyghur Human Rights Policy Act.

Toward that end, I would note that in October of this year BIS added eight Chinese tech companies in the video surveillance, facial/voice recognition, cybersecurity, and artificial intelligence/machine learning sectors to its Entity List, effectively banning these companies from receiving U.S. products and technology without a license. Similar to the restrictions imposed on Huawei and a number of its affiliates starting in May of this year, a license now will be required to export all items subject to the Export Administration Regulations (EAR)—including commercial U.S. hardware, software, and technology—to the companies identified.

Additionally, the Xinjiang Uyghur Autonomous Region (XUAR) People's Government Public Security Bureau, 18 of its subordinate municipal and county public security bureaus, and another subordinate institute were added to the Entity List for what the BIS notice describes as "human rights violations and abuses in the implementation of China's campaign of repression, mass arbitrary detention, and high-technology surveillance" against minority groups in the XUAR. The same restrictions described above apply to these government entities.

Q.2. Can you conceive of any circumstances under which it would be appropriate for the United States to weaken our export control laws and regulations, or the enforcement of those laws and regulations, *vis-a-vis* China or any foreign competitor in order to extract concessions or other commitments from that foreign competitor on matters related to trade or human rights? Please explain your view.

A.2. The strong enforcement of our trade and export control laws is an imperative. This Administration has continued to demonstrate vigilance in the application of these laws to a high degree. For trade matters, any relaxing of the application of such laws and regulations would be done where the United States reaches agreements that bring greater benefits to our national and economic security.

Q.3. In your written testimony, you observed that "the key to ensuring that [Commerce Department's Bureau of Industry and Security] and other export control agencies are able to carry out their missions and the new responsibilities under ECRA is additional funding and resources. If we are serious about addressing the current and future loss of U.S. emerging and foundational technology, if we want to ensure that the United States continues to be a global leader for innovation, security, and freedom, it is critical that such funding and resources is provided." What additional funding and resources would you prescribe?

A.3. For BIS, funding could be provided for more end-use checks to be conducted per annum based on past performance, and BIS could use help on targeting of end-use checks in Hong Kong through upfront research on no license required shipments prior to post-shipment verification requests, enhanced and continued intelligence sharing within BIS, and the utilization of intelligence information to help identify appropriate end-use checks, among other considerations.

Q.4. In your written testimony, you observed that "it is important that we have a system where R&D works here in the United States, but also that key technology does not leave our shores, especially where there is a national security/military nexus." The discussion around export controls focuses significantly on China and other external challenges, but I want to further explore the domestic policies that we can pair with our export control laws in order to drive innovation here at home. Do you believe that significant increases in federally funded basic and applied research could be complementary to our efforts to address controls on emerging and foundational technologies? Please explain your view.

A.4. On August 30, 2019, the Trump administration issued its "Fiscal Year 2021 Administration Research and Development Budget Priorities." In its memo, the Administration states that "While the private sector funds and performs the majority of U.S. R&D, the Federal Government has an important role in funding R&D in areas that industry does not have a strong incentive to invest in and in areas of critical importance to national and economic security." I fully agree with that. Further, the Administration has prioritized Federal R&D funding into "Industries of the Future," such as artificial intelligence and quantum information science.

These industries include emerging and foundational technology. Thus, prioritizing Federal R&D funding toward these sectors will help to build our capabilities and innovations in the sectors that include emerging and foundational technology. Addressing controls of these technologies is a separate funding need, meant for enforcement of our export controls.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM NOVA J. DALY

Q.1. You suggested in your testimony that the United States could implement an "Intellectual Property Entities List," similar to the United States Trade Representative's Notorious Markets List.

Could you elaborate on that idea, and how such an entities list would differ from the Notorious Markets List? What kind of enforcement tools would you want to see created?

A.1. I am still working through the mechanics of such a regime and would be happy to discuss the matter further with the Senator and/or staff. The broad consideration is to establish an interagency committee that would have the power to apply remedies to repeated IP offender entities to include bans or limitations on certain investments, procurements, U.S. companies doing business with such entities, as well as possible financial sanctions, *etc.*

Q.2. This spring, the Trump administration placed Zhongxing Telecommunications Equipment Corporation (ZTE) and then Huawei on the Commerce Department's "Entity List" for export controls for involvement in activities "determined to be contrary to the national security or foreign policy interests of the United States." In your testimony, you called these actions "necessary and long overdue."

As you noted, Congress has also effectively prohibited the Federal Government from purchasing equipment from Huawei and ZTE. How best can Congress continue to support this national security effort?

A.2. Congress has already done a good deal to address the national security concerns arising from the entities mentioned and the presence of their equipment in the U.S. market. As noted, section 889 of the 2019 NDAA prohibits agencies from procuring Huawei and ZTE equipment. The issue of State and local procurements of Huawei and ZTE equipment remain a concern. Congress can continue to support diligence in oversight of the implementation of section 889. Congress can further promote American economic and military competitiveness while addressing this issue by assisting the Administration with actions and funds that advance U.S. artificial intelligence (AI) development and innovation. The President's American AI Initiative could also use the backing and focus of Congress. Continuing to support America's decades-long leadership in AI research and development will increase national security while growing innovative industries and creating cutting-edge, transformative technologies.

Q.3. Do you believe that this action will be disruptive to American manufacturers that supply components to these companies, and if so, do you think there is any way we should address the collateral economic impact?

A.3. There are both positive and negative impacts on U.S. manufacturing and the supply of components as a result of the implementation of section 889 of the NDAA. For this reason, it is important to also ensure that the application of export controls continues to be targeted and surgical. Many State and local providers who have equipment from these entities and who contract with Federal agencies will need assistance. Congress must be ready, where appropriate, with funding to ensure that these State and local entities can address the economic consequences of the law and avail themselves and their systems with other technologies from trusted parties.

Q.4. You said in your testimony you believe the only area for effective export control is computing hardware, which will require multilateral collaboration with countries that have a large amount of hardware engineering expertise. Which countries do you believe are most pivotal for the United States to work with in this regard?

How should Congress and U.S. Departments and agencies decide which computing technologies should be subject to export controls, and which should be areas where free and open exchange of technology could contribute to the greater good?

A.4. Thank you for this question. I believe, however, that Dr. Ben Buchanan in his opening statement testified on this matter. As such, this question would be better answered by him or someone with similar expertise.

Q.5. The rapid development of artificial intelligence brings exciting possibilities. While it is important to safeguard our technology, collaboration with global partners could help bring mutually advantageous developments in the field.

Do you believe there is space to collaborate with China on AI?

A.5. This is an important question with difficult answers. Currently, U.S. companies do collaborate with Chinese entities on AI technologies due to global manufacturing and supply chains. Many U.S. companies manufacture in China. However, given China's theft of intellectual property and other actions, it is imperative that we deeply assess where and the degree to which we have and continue to have such collaboration. We must ensure that the United States and U.S. companies gain long-term benefit from any such collaboration.

RESPONSE TO WRITTEN QUESTION OF SENATOR SINEMA FROM NOVA J. DALY

Q.1. There appears to be consensus that a multilateral approach to export controls is most effective in mitigating technologies that threaten U.S. industry and national security. It also appears there is a consensus that multilateral efforts will work best in restricting divisive Chinese technology and infrastructure. Given the importance of a multilateral approach and the serious national security threats China poses, are you at all concerned that the Administration's policies and rhetoric on trade could undermine the necessary goodwill to work collaboratively with our trading partners to hold China accountable?

A.1. Collaboration with our international allies is always the best response to address bad actors where it concerns the protection of intellectual property. However, trade tensions between the United States and its allies have arisen under nearly all Administrations. One need only look at the yearly "National Trade Estimate Reports on Foreign Trade Barriers" issued by the United States Trade Representative to see that we have had market barrier issues arising from allied countries going back many years. While this Administration has taken a stronger stance on addressing these issues, the United States and its allies have historically found ways to work to address trade tensions. So long as we hold in common the principles of freedom, democracy, and the rule of law, the United States and its allies will continue to find common ground on matters of free and fair trade and also address together the negative aspects of China's lack of IP enforcement and technology theft.

RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN CRAPO FROM BEN BUCHANAN

Q.1. *Big Data and AI*—I know this is a little off topic, but the Banking Committee held three hearings on privacy in the "big data" era, including how data is used to segment, score or otherwise make predictions about an individual's creditworthiness, employability, or general reputation. AI is at the center of this discussion and I am concerned with the extent to which individuals' data is collected and processed without their knowledge, consent, or any real understanding of use or scope. I believe individuals should have rights over their data, including to access, control, correct and delete it.

How do AI systems complicate or challenge the ability of individuals to exercise data rights?

A.1. AI systems enable much better analysis of data. In this sense, they increase the incentive for corporations to collect, store, and examine data on wide swaths of Americans. Simply put, deeper analysis is possible now than ever before because of AI, much of it outside of the view of Americans.

Q.2. What risks are associated with AI in this context and how can they be mitigated in any future legislative effort?

A.2. One substantial risk is that consumers do not understand the way in which their data is being used to draw inferences, via machine learning technology, about them. These inferences, such as their buying preferences, can then be used to drive advertising campaigns. While this risk has long existed, machine learning technology and the associated rise of data analytic tools amplifies it tremendously. While I do not have specific legislation to propose, it seems to me that Congress might investigate whether consumers are meaningfully consenting to the way in which their data is being used.

Q.3. *Google Data Privacy*—Your testimony describes export controls as relatively ineffective in stopping the export of algorithms given the rate of innovation and the fact that AI is a fairly open resource. You also identify the mass of personal and behavioral data as the competitive advantage for large technology companies,

as opposed to their AI systems. It would seem to me then that that data could also be the real vulnerability, if for instance, a foreign adversary were to obtain all of Google's consumer data.

These companies are incentivized to secure their systems, but that may not be enough. My question then is what comprehensive privacy controls or practices could help mitigate the risk of big data being used in this way?

A.3. It is important to differentiate between privacy and security. In general, I think top-tier tech companies like Google have adequate incentive to secure their systems; other companies do not take security nearly seriously enough, as many years of breaches have obviously shown. When it comes to privacy, the risk is not that a foreign hacker will access the data—a security concern—but that the company itself will misuse the data in a way that the consumer does not understand or permit. As I indicated in my answer above, I think that is a very serious risk, and the capability of machine learning systems for ever-deeper analysis amplifies it further. It is vital that American consumers understand what is happening and consent to the terms when they interact with modern technology companies.

Q.4. The United States has a special treatment arrangement with Hong Kong with regards to export controls. While it is in the United States interests to have a strong economic relationship with Hong Kong, there is a lot of concern about growing Chinese encroachment on Hong Kong's autonomy and the potential implications for safeguarding technology.

Is our current export control policy equipped to deal with risk of diversion from Hong Kong to China?

What are some ways in which China is using or could use Hong Kong as a vector for acquisition of technology that we do not export to the Mainland?

What are your specific recommendations for strengthening our export control regime in relation to these challenges?

A.4. Unfortunately, I do not claim any regional expertise on Hong Kong or its relations with China. I have never studied these subjects in any kind of depth, nor am I familiar with how export controls apply to Hong Kong. I must defer to other experts on these three questions as a result.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARREN FROM BEN BUCHANAN

Q.1. At least one U.S. company has been found to have provided the Chinese government with a tool enabling it to monitor Uyghur and Central Asian minorities, as part of what one Uyghur activist described in April 9, 2019, testimony to the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy as "an Orwellian mass surveillance State" where "more than one million Uyghurs are arbitrarily detained outside the legal system in concentration camps." A bipartisan group of Senators introduced the Uyghur Human Rights Policy Act, of which I am a cosponsor, which states in part, that:

> the Secretary of Commerce should review and consider prohibiting the sale or provision of any United States-made goods or services to any state agent in Xinjiang, and adding the Xinjiang branch of the Chinese Communist Party, the Xinjiang Public Security Bureau, and the Xinjiang Office of the United Front Work Department, or any entity acting on their behalf to facilitate the mass internment or forced labor of Turkic Muslims, to the "Entity List" administered by the Department of Commerce.

Do you agree? Please explain your view.

A.1. While it is difficult to know with certainty what is happening in Xinjiang, and while I do not claim particular expertise on the subject, I have certainly read a number of news reports that are both credible and alarming. Like you, I am very worried about the role of technology in aiding repression around the world. I do not think it is appropriate, nor should it be legal, for American companies to aid authoritarian regimes in any effort to crack down on dissent, prosecute religious or ethnic minorities, or otherwise repress their populations.

Q.2. Can you conceive of any circumstances under which it would be appropriate for the United States to weaken our export control laws and regulations, or the enforcement of those laws and regulations, *vis-a-vis* China or any other foreign competitor in order to extract concessions or other commitments from that foreign competitor on matters related to trade or human rights? Please explain your view.

A.2. As I have indicated in other answers, my view is that export controls put in place for national security concerns should not be negotiated away for trade concessions. Doing so undermines the credibility of American export controls.

RESPONSE TO WRITTEN QUESTION OF SENATOR SINEMA FROM BEN BUCHANAN

Q.1. There appears to be consensus that a multilateral approach to export controls is most effective in mitigating technologies that threaten U.S. industry and national security. It also appears there is consensus that multilateral efforts will work best in restricting divisive Chinese technology and infrastructure. Given the importance of a multilateral approach and the serious national security threats China poses, are you at all concerned that the Administration's policies and rhetoric on trade could undermine the necessary goodwill to work collaboratively with our trading partners to hold China accountable?

A.1. Yes, as I indicated in the hearing, I am concerned that the rhetoric and policies of the trade negotiations can, for a variety of reasons, undermine the real and perceived importance of national security concerns. In my view, export controls put in place for national security reasons are not something to be negotiated away, since doing so undermines their credibility of the stated national security concerns. Further, I believe export controls are most effective when done in a multilateral fashion, and any effort to weaken American alliances undermines the potential for strong export controls.

Additional Material Supplied for the Record

July 17, 2019

The Honorable Mike Crapo (R-ID)
Chairman
Senate Banking Committee
538 Dirksen Senate Office Building
Washington DC 20510

The Honorable Sherrod Brown (D-OH)
Ranking Member
Senate Banking Committee
538 Dirksen Senate Office Building
Washington DC 20510

Dear Chairman Crapo and Ranking Member Brown:

Thank you for holding a hearing to discuss implementation of the Export Control Reform Act. As an American technology company, KLA is particularly interested in the efforts underway at the Bureau of Industry and Security (BIS) to define emerging and foundational technologies and implement export controls on sensitive items.

KLA Background

KLA is an American technology company and global leader in process control and process-enabling solutions. KLA makes complex equipment for measuring and inspecting semiconductor devices during development and manufacturing.. KLA is headquartered in Milpitas, California and recently announced a second corporate campus in Ann Arbor, Michigan. We maintain 20 offices in the U.S., including ten U.S. manufacturing facilities in Milpitas, CA; San Diego, CA; San Jose, CA; Tempe, AZ; Ann Arbor, MI; Austin, TX; Oak Ridge, TN; and Lowell, MA; Westwood, MA; and Allentown, PA. KLA has 2,800 U.S. employees and more than 10,000 global employees. In 2018, KLA generated annual revenue of $5.3 billion, of which roughly 15 percent is reinvested in research and development ($2.7 billion invested in R&D since 2015).

KLA's industry leading research has led to advancements in electron and DUV/UV optics, high speed data processing, precision motion control, illumination systems, advanced algorithms, image sensors and computational lithography. KLA serves customers around the world and works to attract the best and brightest talent to help drive innovation.

Global Competitiveness

The semiconductor industry is global and highly competitive. KLA faces increasing competition from foreign companies, with at least two and as many as five foreign competitors in each of its product lines. Companies in Korea, Japan, the Netherlands, Germany, Hungary and China are competing with KLA and its American competitors (e.g. Applied Materials, Rudolph Technologies) to sell to the semiconductor manufacturers across the globe that fuel today's most innovative products.

U.S. Leadership, National Security, and Export Controls

U.S. leadership in innovation and U.S. national security have been closely linked throughout American history. The American semiconductor industry has—without question—been instrumental to the continued leadership of the U.S. military and national security apparatus. Vital to continued U.S. leadership in semiconductors is a responsible U.S. export control system that reflects today's threats and technological capabilities.

We applaud Congress for updating our U.S. export control statute to reflect the strong belief that "the national security of the United States requires that the United States maintain its leadership in the science, technology, engineering, and manufacturing sectors, including foundational technology that is essential to innovation. Such leadership requires that U.S. companies are competitive in global markets."

Economic Considerations

Historically, the U.S. government has carefully crafted export control policy for semiconductors and related technology that appropriately considers the global nature of the industry's supply chain and its impact on the national security of the U.S. As passed in the Export Control Reform Act of 2018 (ECRA), Congress affirmed the importance of including economic considerations in the decision making process, clearly stating that "export controls should be used only after full consideration of the impact on the economy of the United States and only to the extent necessary" to restrict the export of items for national security or foreign policy reasons.

The updated law, which also calls for new controls on emerging and foundational technologies, appropriately recognizes that controls harming the U.S. economy could also harm U.S. military leadership. In the case of KLA, export controls that restrict sales to China would likely lead to a revenue loss of $2 billion, which in turn would reduce KLA's ability to invest in research and development by $350 million over three years, slow down at least five leading edge product development programs, and lead to more than 200 R&D and engineering jobs lost in the U.S. While KLA's customers are diverse, the R&D and technological leadership of KLA and other American semiconductor companies and suppliers help ensure America remains at the forefront of innovation.

Additionally, export controls that are imposed unilaterally will hurt only American companies like KLA. Foreign competitors can and will step in to provide the services and equipment lost to America's restricted presence in the global semiconductor market.

Conclusion

It is critical that BIS and the Administration move forward in a targeted manner that is consistent with the requirements set forth in ECRA. With respect specifically to foundational technologies, the law calls for consideration of three factors: (1) the availability of the technology in foreign countries; (2) how export controls might impact the development of such technologies in the U.S. and (3) the effectiveness of export controls on limiting the proliferation of the technologies to foreign countries. Given these three factors, KLA is urging the Administration to avoid imposing export controls on semiconductor capital equipment as part of the effort to control foundational technologies.

- KLA directly competes with at least two foreign competitors in every product category for semiconductor equipment; the technology is available outside the U.S.
- Export controls imposed on KLA products would lead to U.S. job losses through reduced R&D investment, threatening KLA's leadership position in innovation and in the market.
- KLA's foreign competitors are located in Korea, Japan, the Netherlands, Germany, Taiwan, Israel, Hungary and China. Unilaterally restricting exports on semiconductor capital equipment will not significantly slow the global market or restrict access to these products and services by bad actors.

For these reasons, KLA supports U.S. export controls that remain narrowly focused on national security and foreign policy concerns; are multilateral in nature; and take into consideration the global marketplace and foreign availability of technology.

Thank you for your leadership on these critical issues. We look forward to working with you and your colleagues to ensure the Export Control Reform Act is implemented in a manner that is consistent with the intent of Congress.

Sincerely,

Dennis Ralston

Dennis Ralston
Sr. Director – Government Affairs and Cooperative R&D