Testimony before the Senate Committee on Banking, Housing, and Urban Affairs

"Confronting Threats from China: Assessing Controls on Technology and Investment"

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

June 4, 2019

Chairman Crapo, Ranking Member Brown, and other members of the Committee. Thank you for asking me to testify about and otherwise describe U.S. export controls pertaining to China. Although I am now a partner in the international trade group at Akin Gump Strauss Hauer & Feld LLP, the views I express today are my own. I am not advocating for or against any potential changes to legislation or regulations on behalf of another. Rather, as requested, I am providing you with my thoughts on and understanding of such issues regarding the applicable existing regulations and statutes. My views are influenced by my more than 25 years of work in the area, which includes my service as the Assistant Secretary of Commerce for Export Administration during the Obama Administration.

The topic is a serious one. The United States never wants to be in a fair fight with an adversary. The appropriate, aggressively enforced, clearly written, and well-funded export and related controls are a critical part of maintaining that advantage. They are also a useful tool in helping to achieve U.S. foreign policy, which include human rights, objectives. I have never subscribed to the view that export controls should "balance" national security or foreign policy concerns with economic or trade concerns. National security and foreign policy concerns exist in their own right and are not to be traded off for something else in a particular transaction. The controls should, however, be tailored to specific, identifiable national security threats or foreign policy objectives to avoid collateral economic costs, unnecessary regulatory burdens, and misallocation of federal resources. For the U.S. to be a global leader, our companies need to be successful in the global marketplace. Thus, excessive and over-broad controls -- as a matter of law or perception -- harm the U.S. industrial and technology base, which results in harm to our national security. Lax, out of date, or poorly enforced controls have the same effect. Thus, as a practitioner and a former policymaker in this area, I am pleased that you are holding this hearing and otherwise raising the priority of this complex topic.

With respect to China, the issues pertaining to what the dual-use export control rules and policies should be are the most complex and significant of all export control issues. This has been the case for decades. It is one of our largest trading partners while at the same time being a long-standing country of concern with respect to internal diversion of dual-use items for use in modernizing its military. On the other hand, as I recently described to the U.S.-China Economic Security Review Commission, decisions

involving military items and commercial space-related items destined to China are relatively easy to analyze because of the strict statutory and regulatory embargoes pertaining to such exports and the clear, widely accepted national security and foreign policy reasons for them.

Deciding what the right national security controls should be over commercial items that are not specific to military applications with respect to China (or any other country) ultimately boils down to how one defines "national security." The traditional definition begins with national security experts regularly identifying the commodities, software, and technologies that could give an adversary a military or intelligence advantage or cause us to lose ours. The process also includes identifying the commercial items that are required for the development, production, or use of weapons of mass destruction, particularly missiles, chemical/biological weapons, and nuclear explosive devices. Then, experts in each technology area work backwards from the identified threat to describe the technical characteristics of commercial items necessary for the development, production, or use of such items. Regulators, in a well-established interagency process, then work to add the items to the regulatory control lists of the United States and its multilateral regime allies. This work is done in coordination with industry -- through both advisory committees and notice and comment processes -- to avoid unintended impacts and to ensure clarity. Affected entities in the U.S. and abroad (because U.S. controls are extraterritorial) then adjust their internal compliance programs so that they know when authorization is needed to export such items. When a company wants to ship a listed item (or release a controlled technology to a foreign person), then regulators review its request to do so in the form of a license application. The regulators, as part of a well-tested interagency process, determine whether the export or release would be consistent with our national security and foreign policy objectives. That is, they assess, with the use of intelligence community resources as necessary, whether the item is destined for an acceptable end use or end user, or whether there is a risk that it would be diverted to an unacceptable end use, end user, or destination. They respond accordingly in the form of a license, a denial, or a license with conditions. Enforcement officials investigate and punish violations of the rules and to ensure or motivate compliance. The process must constantly evolve because technologies and threats are constantly evolving.

Another definition of "national security" includes trade policy considerations and sees China's economic ambitions in a wide variety of economic sectors, particularly those described in its Made in China 2025 plan, as a *per se* and long-term threat to the economic health of the United States. Technologies that would support the development of such efforts should therefore be controlled, even if they cannot be tied to a specific military or intelligence application. Export controls should be used to have an impact on the economic viability of foreign companies that compete with U.S. companies. Demand in China for the technologies grows more quickly than regulations and multilateral controls can be updated, meaning that unilateral controls should be used more often. These views, combined with the general and state-supported effort within China to find military applications for dual-use technologies, warrant broader than the traditional considerations over the types of items that should be controlled for export

to China and what the licensing policies should be.

I am not here today to challenge or pick a fight over anyone's particular world view or perspective on how global economics work. Others are much more qualified than me to explain the benefits and costs of industrial policy, comparative advantage, and barriers to trade. I am not denying the extremely serious issues pertaining to Chinese state-supported economic espionage, intellectual property theft, diversion of civil items for military applications, and forced technology transfer. I am also not denying that China's civil-military fusion policies, among other things, make many end-use commitments questionable and force more aggressive review of applications to export controlled items to China. I agree that it is massively hard for regulations to keep pace with the evolution of technology and to get consensus with our allies with respect to matters involving China. What I can do, however, is to describe what, based on decades of experience, export controls can and cannot accomplish *regardless* of one's world view on these issues or other China-specific concerns. In sum, my main general point today is that the application of export controls in ways that are unclear, unpredictable, or unilateral generally ends up harming the very interests they were designed to protect.

I believe that a mature and sophisticated understanding of what export controls can and should accomplish is codified in the recently passed Export Control Reform Act of 2018 (ECRA), which I will also describe. It is an excellent piece of bi-partisan legislation that probably can be the authority to address just about any problem that export controls can address, including those involving China. It is a modern, coherent, and permanent authorization for not only list-based controls (*i.e.*, over the export of identified items), but also end-user-based, and end-use-based controls as part of a three-legged stool approach to achieving national security and foreign policy objectives. Congratulations to this Committee, its staff, its House counterparts, and the Administration in getting it through along with related improvements to the laws governing foreign direct investment.

ECRA is, however, quite new. Indeed, the regulators have not even finished the process for drafting implementing regulations, such as those with respect to possible new controls on exports to China (section 4818) or on emerging and foundational technologies that are not now controlled but should be given China-related concerns (section 4817). Thus, although it is not my job to tell Members of Congress how to do theirs, my suggestion and request for the greater good would be for Congress to provide substantially more financial and other support for and oversight of the agency responsible for shepherding all this activity, the Commerce Department's Bureau of Industry and Security (BIS). It is a terrific little agency with great people that punches way above its weight. Never before though have the issues over which it is responsible been more complex, fast-moving, and consequential – particularly with respect to issues involving China. It, thus, needs significantly more resources than it has now to do properly all the jobs given to it by ECRA, other laws, new Executive Orders, and the Administration. Also, BIS has not been for decades subject to as many statutory standards for what it should and should not do with respect to export controls as is now the case with ECRA. Thus, a vital requirement for successful export control policy is for

this Committee and the House Foreign Affairs Committee to regularly ensure that ECRA is being faithfully implemented.

Export Controls and the Primary Agencies That Administer Them

Before I dive in to China-specific issues, it is important to level set for everyone that export controls are the rules that govern

(i) the export, reexport, and (in-country) transfer
(ii) by U.S. and foreign persons
(iii) of commodities, technology, software, and, in some cases, services
(iv) to destinations, end users, and end uses
(v) to accomplish various national security and foreign policy objectives, including human rights objectives.

This one sentence summary is deceptively simple. As much as this and previous administrations try to make the rules easy to understand and apply, they are inherently complex from an industry perspective. From the policymakers' perspective, each export control decision require multivariate policy and legal analyses involving statutes, regulations, international commitments, intelligence and law enforcement equities, intelligence community threat assessments, industrial base implications, license administration, budgets, available technical expertise, corporate compliance program considerations, foreign availability, interagency dynamics, how global production and supply chains work, congressional concerns, multilateral and bilateral foreign policy issues, and, in the end, largely subjective assessments of what constitutes a national security or a foreign policy concern with imperfect information that can be addressed through regulating the movement of commodities, technology, software, and some types of activities.

The technologies are often evolving and wide ranging, including everything from information about bird flu to machine tools to items that are being invented today that most do not understand. Specific commodities, such as certain types of microwave monolithic integrated circuits, that are critical to advanced military radar are equally critical to modern telecommunications applications. Technologies that were once sensitive become ubiquitous, such as the GPS technology in our cell phones. Generally non-sensitive commercial technologies can, however, be applied to new uses or by end users of concern in ways that are harmful to our interests. Most extraordinarily advanced technologies, however, represent no threat whatsoever. Many simple, old technologies, such as those unique to standard military equipment, warrant controls for most of the world. Concerns about destinations, end users, and end uses vary widely and change constantly. The mere existence of a control, and the internal obligations that go with it, can sometimes do more harm than good even if the regulators would generally approve transactions under its authority.

The Export Control Reform Act of 2018

I described the U.S. export control system in more detail to the House Foreign Affairs Committee during its consideration of what eventually became ECRA. I incorporate those comments by reference. ECRA is the new authority for the Export Administration Regulations (EAR), which BIS administers. Although BIS leads the dual-use export control system, ECRA, Executive Orders, and regulations require significant interagency cooperation on licensing policies and decisions, primarily with the Defense Department on national security issues and the State Department on foreign policy issues.

Until ECRA, the statutory authority for the EAR – the Export Administration Act of 1979 – had lapsed decades ago. The EAR were kept in effect through a series of Executive Orders and emergency declarations issued under the authority of the International Emergency Economic Powers Act. Thus, for decades, Congress had not expressed a coherent vision for what export controls should be designed to accomplish. Although there were certainly basic good government reasons motivating ECRA's introduction and passage, we basically have bi-partisan concerns regarding Chinese investment strategies and efforts to acquire dual-use technologies for use in modernizing its military to thank for bringing Congress together on this issue.

As you know, in late 2017 and the first half of 2018, there was a non-partisan effort to reform and expand the jurisdictional authority of the Committee on Foreign Investment in the United States (CFIUS), largely in response to national security concerns pertaining to investments in the United States from China. One of provisions in the Foreign Investment Risk Review and Modernization Act (FIRRMA) as introduced would have given CFIUS jurisdiction over some types of outbound investments by U.S. critical technology companies in foreign countries in order to regulate the transfer of currently uncontrolled emerging and foundational technologies that, with more analysis, warranted controls. I and many others, including many on this Committee, said that such concerns were warranted, but that addressing them through CFIUS both under-controlled and over-controlled. It under-controlled because the government's review would only be triggered with a covered transaction. If the U.S. Government should regulate the transfer to China or elsewhere a newly identified sensitive technology for national security reasons then it should regulate the transfer of such technology regardless of the nature of the underlying investment. I and many others pointed out that the U.S. government already had a regulatory system and an interagency process in place to identify and control technologies of concern – the dual-use export control system BIS administers.

That policy debate is what led to ECRA's being the legislative vehicle for addressing the identification and control over transfers to countries of concern such as China of emerging and foundational technologies. This then led to an opportunity for Congress to finally implement permanent statutory authority for the EAR, to articulate a modern vision for export controls, enhance export control enforcement authorities, and to codify in law decades of BIS practice, policies, and regulatory reforms – including the Obama Administration's Export Control Reform accomplishments. The rules regarding foreign

investment in the United States and export controls are now connected and overlapping to address, among other things, policy concerns over the release to foreign persons in the U.S. and abroad of the technologies to be identified. In sum, CFIUS uses its authority over *inbound* investment to address concerns, *inter alia*, regarding transfers of potentially sensitive uncontrolled technologies to foreign persons. The EAR focus on *outbound* activities (and releases to foreign persons in the United States of controlled technology) to address technology transfer concerns regarding identified technologies. Emerging and foundational technologies added to the EAR's list of controlled items -- the Commerce Control List (CCL) -- will simultaneously expand CFIUS's jurisdiction over foreign investments in the U.S. involving such technologies.

As I and many others could describe separately, the Treasury Department is leading the effort to draft the regulations to implement FIRRMA, *i.e.,* the new rules expanding CFIUS's authority to regulate foreign investment in the United States that might create unresolved national security issues. From conferences, I understand Treasury plans to publish proposed rules later this year. Because Commerce has not yet published proposed rules implementing ECRA provisions (such as those pertaining to controls over emerging or foundational technologies) and Treasury has not published new rules implementing FIRRMA provisions (such as those pertaining to non-controlling investments in critical infrastructure), I cannot comment on them. With respect to ECRA, I can, however, provide the context for the issues to help you and others evaluate the proposed rules once they are published.

Emerging and Foundational Technologies – Identification and Control Efforts Motivated Largely by Concerns Pertaining to China

Understanding that the bar for the imposition of unilateral controls should be high, Congress set out in ECRA clear statutory standards governing the effort to identify and control emerging and foundational technologies – again, largely in response to concerns raised by efforts by Chinese companies to acquire such technologies and use them in ways contrary to U.S. national security interests. Specifically, ECRA section 4817(a) requires the Administration to conduct an interagency effort that reaches out to all available sources of information -- including academia, industry, and the intelligence community -- to identify emerging and foundational technologies that "are essential to the national security of the United States" and that are not now subject to a multilateral control in the EAR's CCL or described on one of the other lists of technologies the U.S. controls for export.[1] Once such technologies are identified, ECRA requires BIS to get industry input on the controls in response to a proposed rule. Such comments must then be considered, consistent with the standards in ECRA, before BIS imposes any final controls on the newly identified technologies.

[1] Even before ECRA, BIS had the authority to impose unilateral controls over technologies that warranted control. We created a process for doing so in 2012 – the "0y521" process. ECRA's emerging and foundational technology provisions are largely based on this process. The difference, of course, is that ECRA section 4817 expresses the will of Congress and made the effort mandatory as opposed to discretionary.

Although ECRA does not define "national security," a request for comment BIS published in November 2018 described the national security concerns to be addressed by the effort, *i.e.,* to identify now uncontrolled items that "have potential conventional weapons, intelligence collection, weapons of mass destruction, or terrorist applications, or [that] could provide the United States with a qualitative military or intelligence advantage."[2] These examples track ECRA's definition of a "dual-use" item, which is an item that has "civilian applications and military, terrorism, weapons of mass destruction, or law-enforcement-related applications." Given the broad controls that already exist in the EAR over items specially designed for military applications that are not controlled by the International Traffic in Arms Regulations, and all technology at any stage required for their development or production, I am not certain what now-uncontrolled items meet this definition. That is, however, what the ECRA section 4817 process is designed to discover in a regular-order, transparent fashion.

In deciding whether to identify such a technology as "emerging" or "foundational" and impose unilateral controls on its export, reexport, and in-country transfer, ECRA section 4817(a)(2)(B) requires the Administration to take in to account the:

(i) development of the technologies in foreign countries;

(ii) effect export controls imposed pursuant to this section may have on the development of such technologies in the United States; and

(iii) effectiveness of export controls imposed pursuant to this section on limiting the proliferation of emerging or foundational technologies to foreign countries.

BIS has recently implemented multilateral controls on emerging technologies that are essential the national security of the United States. (The new controls pertain to discrete microwave transistors, software operations, post-quantum cryptography, underwater transducers, and air-launch platforms.) Licenses are required to export such items to China and most other countries. BIS officials have said publicly that it and its export control agency colleagues continue work on identifying additional such technologies for consideration as either unilateral or multilateral controls. This makes sense because ECRA requires the effort to be an "on-going" one. That is, contrary to many comments I have heard, ECRA does not contemplate a one-time publication of

[2] BIS stated in its notice that it is not attempting to "expand jurisdiction over technologies that are not subject to the EAR." EAR section 734.3(b)(3) states that the following types of information are not "subject to the EAR," regardless of their content: (i) "published" information; (ii) information that arises during, or results from, "fundamental research;" (iii) information released by instruction in academic institutions; (iv) information in patents and published patent applications; (v) information that is a non-proprietary system description; and (vi) certain types of telemetry. Each of these elements of the regulatory exclusion is further defined in this and related EAR provisions. BIS presumably made this point to allay concerns by some, particularly in the academic and research communities, that BIS's effort to identify and control emerging and foundational technologies might somehow affect the long-standing uncontrolled status of published information and fundamental research.

new unilateral controls on emerging and foundational technologies.

The technology areas BIS announced that it is studying dovetail with those China announced in its Made in China 2025 plan as those of strategic significance for the country. According to BIS, they include:

- "Biotechnology"
- "Artificial intelligence (AI) and machine learning technology"
- "Position, Navigation, and Timing (PNT) technology"
- "Microprocessor technology"
- "Advanced computing technology"
- "Data analytics technology"
- "Quantum information and sensing technology"
- "Logistics technology"
- "Additive manufacturing (e.g. 3D printing)"
- "Robotics"
- "Brain-computer interfaces"
- "Hypersonics"
- "Advanced Materials"
- "Advanced surveillance technologies"

For each technology identified in a proposed rule to be controlled as "emerging" or "foundational," ECRA essentially imposes on BIS a burden of justifying why the proposed control meets several statutory standards. Thus, for example, ECRA essentially requires BIS to demonstrate

(i) why the technology proposed to be controlled is "essential" to U.S. national security;

(ii) what the specific weapons-, military-, or intelligence-related application the control is designed to address that is not now being addressed by a control;

(iii) why the unilateral control would not harm domestic research in the technology;

(iv) why the rule would be effective at stemming the proliferation of the identified technology to countries of concern such as China (taking into account any foreign availability of the same technology); and

(v) the results of BIS's full consideration of the impact on the U.S. economy that would result from the unilateral control.

Without such information, industry and this Committee would not be able to provide useful comments or oversight consistent with the standards and goals of ECRA.

If BIS imposes controls on such technologies, or subsets thereof, ECRA requires the Administration to work to get a multilateral regime to agree to the same control so that the United States is not alone in the control. This effectively means that any proposed control should be of a type that is consistent with, and would likely be accepted by, the relevant multilateral regime. Proposing a control over an item inconsistent with what a regime would accept would defeat the point of this ECRA provision and the high bar ECRA places on the use of unilateral controls for emerging or foundational technologies. In any event, as evidenced by industry comments, such multilateral efforts are vital to ensuring that the controls are effective and that U.S. companies are not put at an unfair competitive disadvantage relative to its competitors in allied countries.

Industry comments on the process were due on January 10, 2019. They seem to be largely concerned that unilateral controls on commercial technology available outside the United States would harm U.S. industry. That is, such controls would merely drive demand for such commercial technologies to non-U.S. countries. This would harm the ability for companies in the United States to invest in the R&D necessary to advance such technologies while enhancing the ability of companies outside the United States to do so. Another concern was that unilateral controls over such technologies would be ineffective because, given the international development of the broad categories of technologies identified, they would not deprive China of the ability to develop or acquire the same capability from elsewhere. Many commenters, therefore, asked BIS not to adopt any new controls on such technologies until and unless they were agreed to by one of the relevant multilateral regimes.

Industry also largely did not know how to respond to BIS's requests for comments regarding what industry thought were now uncontrolled technologies essential the national security of the United States. Industry essentially offered information on foreign availability, asked BIS to abide by the ECRA standards, and asked to be included in the drafting efforts to ensure clarity and precision. Many comments, however, said that it was the government's job to identify the national security threats that were not now being addressed but should be, not industry's. BIS has not responded to the comments, probably because it is still working through the issues with its interagency colleagues. It also has not yet issued a notice asking for similar industry comments on which "foundational" technologies should and should not be controlled.

Going back to my polite request for more resources for BIS, this effort is vastly more difficult and resource-intensive than anything we did during the Export Control Reform effort. It was relatively easy to comprehend technology to develop a military aircraft's landing gear (and hundreds of thousands of other similar components), for example, and change its jurisdictional status to enhance military interoperability with our NATO-plus allies. It is radically harder to comprehend technology related to quantum computing, for example -- and even harder to sort out the subsets thereof essential to U.S. national security that are even capable of being controlled given its cross-border development. It was also much easier for us to assess the economic impacts of changing the jurisdictional status of less sensitive military items than it will be for BIS to

gather the ECRA-required information from industry to assess the economic impact of a unilateral control, even a short-term unilateral control that might later be submitted to a multilateral regime. Such assessments must take into account not only the loss of actual sales but also the long-term impact on foreign customers and whether they will consider U.S. companies to be unreliable suppliers and thus move their business to non-U.S. manufacturers.

If the Trump and subsequent administrations strictly follow the ECRA standards, then any new controls will only be over a small list of non-mature specific technologies that are essentially unique to the United States, not currently export-controlled, and truly essential to the national security (and thus should have been controlled under any administration even without the section 4817 effort). I do not know what will happen with respect the first group of proposed new controls under ECRA, but I do know that industry in potentially affected industries is extremely interested in whether their commercial technologies will become subject to unilateral controls or a tool of trade policy. Companies are or will be making decisions on whether to invest or not invest in the United States based upon a belief or fear, rational or otherwise, that technologies in various commercial sectors will or will not be able to be shared, jointly developed, and sold.

ECRA States that Export Controls Exist to Accomplish National Security and Foreign Policy Objectives

Industry's concern, at least in my experience, that export controls not become a tool of trade policy is echoed by ECRA's statement of policy for why U.S. export controls exist. Specifically, section 4811(1) states that the United States should "use export controls only after full consideration of the impact on the economy of the United States and only to the extent necessary – (A) to restrict the export of items which would make a significant contribution to the military potential of any other country or combination of countries which would prove detrimental to the **national security** of the United States; and (B) to restrict the export of items if necessary to further significantly the **foreign policy** of the United States or to fulfill its declared international obligations."

ECRA's second statement of policy for why U.S. export controls exist is additionally limited in scope to addressing specific, tailored, identifiable national security and foreign policy objectives that do not include trade policy concerns.

> "The national security and foreign policy of the United States require that the export, reexport, and in-country transfer of items, and specific activities of United States persons, wherever located, be controlled for the following purposes:
>
> (A) To control the release of items for use in –
>
> (i) the proliferation of weapons of mass destruction or of conventional weapons;

(ii) the acquisition of destabilizing numbers or types of conventional weapons;

(iii) acts of terrorism;

(iv) military programs that could pose a threat to the security of the United States or its allies; or

(v) activities undertaken specifically to cause significant interference with or disruption of critical infrastructure.

(B) To preserve the qualitative military superiority of the United States.

(C) To strengthen the United States defense industrial base.

(D) To carry out the foreign policy of the United States, including the protection of human rights and the promotion of democracy.

(E) To carry out obligations and commitments under international agreements and arrangements, including multilateral export control regimes.

(F) To facilitate military interoperability between the United States and its North Atlantic Treaty Organization (NATO) and other close allies.

(G) To ensure national security controls are tailored to focus on those core technologies and other items that are capable of being used to pose a serious national security threat to the United States."

Thus, with respect to any new proposed control, ECRA effectively requires BIS to assess and identify to this Committee and the public what the impact on U.S. industry would be as a result of a new control; how it furthers one of the listed objectives; and how it is "tailored" to "focus" on "core" technologies that pose a specific and "serious" national security threat. Nothing about these standards changes because the destination of an item would be China or another country.

Although ECRA does not require specific national security concerns to be compromised to achieve economic objectives, it does state in paragraph 3 of its policy statement 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 United States persons are competitive in global markets. The impact of the implementation of [ECRA] on such leadership and competitiveness must be evaluated on an ongoing basis and applied in imposing controls under [ECRA] to avoid negatively affecting such leadership." Of course, government is the one responsible for making national security determinations, but industry is generally in a better position to assess how or whether a specific export control would negatively affect its global leadership in an area. Thus, their views in response to this statutory requirement of an ongoing evaluation of the impact of export controls should be solicited and given great weight – again, understanding that the government must make the final call on what is in the national security or foreign policy interests of the United States.

This is one area where issues involving China-specific export controls become massively complex and sometimes counter-intuitive. For many U.S. industries, China is one of the largest customers. The companies use the income from such sales to benign end uses and end users to fund their R&D efforts in the United States to advance the next generation of their products. This allows them to remain economically competitive internationally, which thus enhances the U.S. industrial base. Without such sales, the income will go to their competitors outside the United States, which results in companies in the United States becoming less economically competitive relative to foreign competitors and indigenous development in China. This is why I am a firm believer in ECRA's requirement that controls be tailored to specific, identifiable national security threats so that a loss of trade in less sensitive items where risk of diversion is low does not end up harming the U.S. industrial base, which thus harms our national security in more fundamental ways.

ECRA Strongly Favors Multilateral Controls over Unilateral Controls

As discussed earlier, a major concern of industry in response to BIS's request for information about emerging technologies is that BIS would impose unilateral controls – *i.e.,* those that only the United States imposes. Congress had the same general concern when it wrote in section 4811(5) that "[e]xport controls should be coordinated with the multilateral export control regimes. Export controls that are multilateral are most effective, and should be tailored to focus on those core technologies and other items that are capable of being used to pose a serious national security threat to the United States and its allies." ECRA subsection (6) goes on to state that "[e]xport controls applied unilaterally to items widely available from foreign sources generally are less effective in preventing end-users from acquiring those items. Application of unilateral export controls should be limited for purposes of protecting specific United States national security and foreign policy interests." Thus, I am not saying that ECRA prohibits unilateral controls, only that they should be rare and narrowly tailored to address specific national security or foreign policy issues, and imposed consistent with the ECRA standards described earlier.

I realize that one of the motives for the outbound investment provision of FIRRMA as introduced was that the multilateral control process is slow. It requires consensus among between 30 and 40 or so regime partners with many different types of industries

and local concerns. Most of the allies do not have the same concerns with respect to China that the United States does. There are language barriers and other agendas that get in the way. Other countries' enforcement systems for violations are not as robust as ours. I get that. I dealt with it regularly. Process is hard. Short-cut alternatives of easy feel-good unilateral controls, except in extraordinarily narrow and specific circumstances, however, will always end up doing more harm than good for the very industry or technology the control is designed to protect. That is the lesson learned from decades of export control efforts and is true regardless of one's view of global economics or definition of national security. The work and the investments (and thus U.S. jobs) will simply be driven off-shore to allied countries without such controls. Foreign buyers will design-out U.S.-origin content because of the unilateral regulatory burdens that go with it. It's like squeezing a handful of sand too hard; eventually you have none. So, if the multilateral process is too slow, come with other ideas with close allies to speed it up, such as by working with smaller groups of truly interested countries. If they do not have the same concerns regarding China, provide the evidence to convince them. If their enforcement systems are lax, help them build capacity. All such tasks require massive additional funding for BIS and the other export control agencies to implement properly.

China-Specific Licensing Policies in ECRA and the EAR

ECRA did not change any policies regarding exports to China. Section 4818, however, required a review of the licensing requirements pertaining to China and other countries subject to U.S. arms embargos. Section 4818(b) required the results of the review to be implemented by May 10, 2019. I do not know the results of the effort. I know that industry is curious about what the changes will be though. I am not saying that any particular new control is or is not warranted. Rather, I am just reporting that many are wondering what the impact on their businesses will be and how BIS will justify any new controls based on the ECRA standards described above.

ECRA requires that licensing requirements be imposed on exports of emerging and foundational technologies if destined to China or other countries subject to arms embargoes. ECRA leaves to BIS the decision to impose licensing requirements involving other countries. Also, unless BIS changes a core element of the EAR, these licensing requirements will also apply to "deemed exports," *i.e.*, releases of technology in the United States to nationals of countries that have a license requirement, such as China.

In thinking about possible changes in licensing policy with respect to China, it is important to remember that almost all multilaterally controlled items already require a license for export to China and the Executive Branch has wide latitude in deciding whether and when to approve, condition, or deny such licenses. BIS does not make such decisions alone, by the way. They are made in coordination with its colleagues in the departments of Defense, State, and Energy. If there is a disagreement among the agencies, there are formal appeal procedures that have, in the main, worked well for decades. Reports of Defense or State officials being routinely "overruled" by

Commerce officials in final determinations during such procedures are untrue.

The following are additional already-existing China-specific export controls and licensing policies in the EAR. BIS has the authority to impose individual licensing requirements on the export of specific types of otherwise uncontrolled items in a transaction merely by informing the exporter that a national security concern exists with respect to the transaction. The EAR contain absolute and complete embargoes on the export of military and commercial space-related items to China, directly or indirectly. The EAR contain "zero *de minimis*" rules with respect to foreign-made military items, of any significance, and commercial space-related items. This essentially means that a foreign-made item containing any amount of U.S.-origin content specially designed for a military or space-related item requires a license for export from outside the United States, which will be presumptively denied. Wholly foreign-origin items controlled for national security reasons that are the direct product of U.S.-origin technology controlled for national security reasons also require a license from BIS to export to China and other countries of concern. BIS has a process for conducting pre-shipment checks and post-shipment verifications with respect to exports to China and other countries. If the foreign companies do not cooperate, BIS has a process for exerting leverage over the foreign companies to cooperate, which is the Unverified List.

China-Specific Controls Based on End Users

As I mentioned earlier, the EAR can achieve their national security and foreign policy objectives through controls over lists of identified items, specific end-users, or specific end-uses. It is not a one-size-fits all regulation. The EAR essentially have three end-user-based tools, which have often been used against entities in China and other countries. They are (i) the Unverified List (to impose obligations on exports to determine the bona fides of a foreign entity or to allow for an end use check), (ii) the Denied Persons List (to impose punishment for those that have violated the EAR); and (iii) the Entity List. The Entity List is a hot topic these days. It has, however, been a tool for BIS to use for decades. It is just getting much more attention because of the size and scale of the recent listings of Huawei and affiliated entities.

The list has hundreds of entities on it, many of which were added by me in coordination with my interagency colleagues. Obviously, as the one who added ZTE to the Entity List in March of 2016, I believe that it can be an effective tool for accomplishing national security objectives and supporting law enforcement efforts by motivating changes in the behavior of foreign parties engaged in acts contrary to our national security or foreign policy interests – if there is a plan for what is to be achieved with the listing. Indeed, the standard in the EAR for when an entity is to be removed from the list is "if it is no longer engaged in [such activities] and is unlikely to engage in such activities in the future."

Being added to the Entity List is thus not an assessment of a civil or criminal penalty against the listed entity. The burden of proof for listing is lower than even that for a standard civil penalty. The EAR requires only that there be a "reasonable cause to believe, based on specific and articulable facts," that a foreign entity has been involved,

is involved in, or poses a significant risk of being or becoming involved in, "activities that are contrary to the national security or foreign policy interests of the United States." Neither ECRA nor the EAR define or limit what constitutes a "national security" or "foreign policy" interest with respect to the Entity List. The EAR contains an "illustrative list" of "examples" of such activities, such as supporting persons engaged in acts of terror; enhancing the military capability of state sponsor of terrorism; transferring, developing, servicing, repairing, or producing weapons; preventing BIS from conducting an end-use check; and posing a risk of violating the EAR, such by transferring items to proscribed destinations, end uses, and end users. The decision, however, is up to whoever is in charge and the interagency clearance process as described in the EAR.

My view, based on the structure of the EAR and my experience, is that the Entity List tool should be used to change the behavior of foreign entities and not just as a low burden-of-proof tool of punishment. Otherwise, the risk of its being over-used, and thus provoking uncertainty about which entities it might be used against, provokes concerns by foreign buyers that U.S. exporters are not reliable and predictable suppliers. Remember, in international trade, perception is as important as reality and must be managed accordingly. With these comments, I am not challenging any of the recent Entity List actions or saying that a foreign company can be too big to list. Also, I, of course, no longer have access to the same non-public information my successors at BIS have, thus making it hard for me to judge many issues. Rather, I am reporting that, given the recent notoriety of the tool, it is having an impact on otherwise authorized trade with China involving unaffiliated and benign end uses and end users. This effect warrants study so that the mere existence of the otherwise effective tool does not end up doing more harm than good for U.S. industry.

Of course, if a foreign entity has violated the EAR, then it should absolutely be charged and punished consistent with the standards, procedures, and due process set out in the EAR and the relevant criminal code provisions. Moreover, I advocate for more enforcement resources for BIS's Office of Export Enforcement (OEE). OEE is unique among law enforcement agencies in that it is dedicated solely to investigating and assisting in the prosecution of export control cases. Investigating exports and other activities involving China has always been among its top priorities given the diversion risk concerns described earlier. I know that advocacy for more enforcement resources may seem to be a counter-intuitive suggestion from someone now in industry, but robust enforcement helps keep the playing field level for those companies that do the hard work to establish procedures to ensure compliance with the controls.

The EAR prohibit exports of a list of otherwise uncontrolled items to Russia or Venezuela if for a "military end user." Such a "military end user" control with respect to China was not adopted during the Bush Administration because, as a I recall, of the difficulty in identifying such end users when they are engaged in purely civilian activities, such as running hospitals and airports. I, too, was not able to come up with a clear definition of the term that exporters could comply with, but suspect BIS is now working on the issue given the requirements of ECRA to review China licensing policies.

China-Specific Controls on End Uses

The EAR, however, contain a China military end use rule. In essence, it requires an exporter, reexporter, or transferor to apply for a license when it knows that an item on a list of 32 types of items that do not ordinarily require a license for export to China are for a military end use in China. Such items include civilian aircraft engines, navigation systems, certain composite materials, and telecommunications equipment. Applications for such exports will be presumptively denied. BIS also has the authority to inform an exporter that there is an unacceptable risk that an item will be diverted for a military end use in China and that, as a result, the item may not be shipped without a license.

ECRA permits other end use controls. This makes sense because, as previous technology control identification efforts have demonstrated, detailed technical descriptions of specific new technologies for inclusion on control lists can sometimes end up doing more harm than good. If, for example, a technology is the same as that which is used to commit a bad act as is used to defend against the bad act, then a list-based control and all the regulatory complexity that goes with it will harm the defenders far more than the attackers. The solution for when list-based controls would be ineffective, or would do more harm than good, is to focus on the end uses of concern. When someone in government or civil society identifies concerns with such widely available items, the concern is generally more about how they are being used and who is using them than something inherently threatening in the commodity, software, or technology.

Although not exclusive to China, the EAR contain a series of controls on exports, reexports, and transfers related to nuclear, missile, and chemical/biological end uses. As referenced in ECRA and as implemented in EAR section 744.6, the EAR also already control a range of services performed by U.S. persons if with respect to missiles, nuclear explosive devices, or chemical/biological weapons – regardless of whether the items involved in the service are subject to the jurisdiction of the EAR. Although there are no China-specific end-use controls in the EAR or ECRA, ECRA section 4812(a)(2)(F) requires the President to "control the activities of United States persons, wherever located, relating to specific . . . foreign military intelligence services." Congress presumably added this requirement to narrow a gap between the ITAR's controls on defense services and services that do not involve defense articles but still warrant control for national security reasons. BIS has not yet implemented this control in the EAR. When it does, the addition may address some of the China-specific policy concerns I am aware of. I would thus encourage the Committee to study and track the provision's implementation. When I considered implementing a similar idea in the EAR, I was unable to develop a definition of foreign intelligence services that accomplished the policy objectives of the control and that also would be understandable to those who would need to comply with it.

Hong Kong

The United States-Hong Kong Policy Act of 1992 effectively requires the U.S. government to treat Hong Kong and mainland China as two separate destinations for export control purposes. In addition, section 103(8) of the Act states that the "United States should continue to support access by Hong Kong to sensitive technologies controlled under [the then existing multilateral export control regime that is the predecessor to the Wassenaar Arrangement] for so long as the United States is satisfied that such technologies are protected from improper use or export." Because the United States has not made a determination to the contrary, the statutory and regulatory prohibitions pertaining to the export and reexport of controlled items subject to U.S. jurisdiction that are applicable to mainland China do not apply if the destination is Hong Kong. The export control regulations, however, still require licenses to export and reexport controlled items to Hong Kong. Applications for such exports and reexports are reviewed by U.S. government export control authorities to determine, for example, whether Hong Kong is indeed the ultimate destination and whether the export or reexport otherwise presents any national security or foreign policy concerns.

I was asked to comment on whether items subject to U.S. export controls are being illegally exported out of Hong Kong to mainland China or other countries of concern. I left the government on January 20, 2017 and thus no longer have access to such information, whether positive or negative. I can, however, say that on January 19, 2017, a rule that I signed expressing concerns about the issue remains in effect. The rule imposes additional support document requirements on exports and reexports to Hong Kong. In essence, the rule leveraged the EAR to effectively compel compliance with Hong Kong export and import permit requirements by requiring proof of compliance with Hong Kong law as a support document necessary for shipping under an EAR license or license exception. As stated in the preamble, BIS took "this action to provide greater assurance that U.S.-origin items that are subject to multilateral control regimes . . . will be properly authorized by the United States to the final destination [such as mainland China], even when those items first pass through Hong Kong." My thought at the time was that if we had regular, robust assurances and intelligence that diversions of U.S.-origin items were not occurring, then the additional requirements would remain in effect as is or be removed. If not, then the stricter licensing policies, including policies of presumptive denials, would need to be imposed. I would encourage you to ask this question of current BIS officials.

ECRA Authorizes the Tools in the EAR to be Used to Further U.S. Foreign Policy, Including Human Rights, Objectives

Most of my comments pertain to national security issues. ECRA, however, specifically authorizes the EAR to be used as a tool to "carry out the foreign policy of the United States, including the protection of human rights and the promotion of democracy." The EAR also contains an extensive list of foreign policy controls. Items controlled under such policies include crime control and detection equipment, restraints, stun guns, instruments of torture, equipment for executions, and shotguns. Following the 1989

military assault on demonstrators by the Chinese government in Tiananmen Square – 30 years ago today -- the U.S. Government imposed controls on many such items.

All license applications BIS receives to export such and other types of items are reviewed by BIS foreign policy experts and also referred to the State Department for its assessment of the foreign policy and human rights implications. (With one exception involving a complex, atypical fact pattern with national security implications, I am confident that the State Department's assessment that a license should be denied for human rights-related reasons has never been rejected by BIS and the other agencies.) Because, however, the nature of most items involved in acts contrary to this ECRA provision are common or do not lend themselves to technical descriptions on control lists, a combination of the EAR's other end-use- and end-user-based tools could be effective in furthering its objectives. I recognize that the Entity List is not commonly used to further such objectives, but it could be. I make this point only to respond to a likely request to explain the tools in the EAR available to address various human rights concerns.

The Need for Certainty, Clarity, and Multilateralism in Export Control Policy – And How Perception is Sometimes More Important than Reality

As someone who now hears concerns of U.S. industry on a billable hour-by-hour basis, I can report that there is considerable concern that the United States will begin imposing broad controls on the large categories of commercial emerging technologies identified in BIS's November request for information for non-traditional national security reasons. I am not saying controls consistent with ECRA's standards and requirements should not be imposed. Rather, I am just reporting that most companies do not appreciate that BIS's notice was a request for public input and information about broad categories of technologies in order for BIS to use in considering how to develop narrowly tailored controls essential to national security. They also generally do not appreciate that there are specific statutory standards governing the effort and what technologies may and may not be added to the control lists. Because perception can, however, become reality with respect to economic decisions involving U.S. companies, my recommendation is that BIS describe its plans for new China-specific controls publicly with clarity, certainty, and with as much ECRA-consistent emphasis on multilateral solutions as possible. This is vital to reducing uncertainty, and thus unnecessarily lost business opportunities for U.S. companies involving benign items, among those who do not follow the nuances of the EAR, ECRA, and the regulatory process.

I acknowledge this will be difficult even when BIS is ready to publish proposed rules. However, ECRA essentially requires BIS to demonstrate, for example, why any new proposed unilateral emerging technology control is "essential" to national security, why it would not harm domestic research, and why it would be effective at stemming the proliferation of such controls to China and other countries of concern. BIS now, per ECRA, also must fully consider the impact on the U.S. economy that would result from any new unilateral control, an effort that it will need industry's help in doing. These are high standards, but Congress created them because, as stated several times in ECRA,

unilateral controls should be rare and only respond to specific or emergency situations essential to our national security. All other list-based controls are better addressed through the regular order and the well-tested process of working with our multilateral regime partners to develop and implement multilateral controls to enhance their effectiveness and keep the United States on a level playing field with such countries, particularly with respect to commercial technologies.

Conclusion

The United States has always pursued two complementary objectives – protecting our national security and promoting U.S. technology leadership. While they both make us stronger, they have very different tools and purposes. We have spent 50 years building a global trading system with clear rules and tools for remedying unfair trade practices. Export controls are not one of them. If we use export control-related national security justifications for purely trade policy purposes, we will undermine the system we have built and even further encourage the Chinese government to do so even more. Export controls should be used to their fullest possible extent, however, when a specific national security or foreign policy issue pertains to the export, reexport, or transfer of commodities, technologies, software, or services to destinations, end users, or end uses. If the issue pertains to an activity, an investment, or a concern separate from such events or concerns, then one must look to other areas of law, such as sanctions, trade remedies, foreign direct investment controls, intellectual property theft remedies, or counter-espionage laws. In addition, a trade agreement among Pacific allies surrounding China could be a useful tool in motivating, through collective multilateral action, changes in unfair Chinese trade activities – while, at the same time, benefiting U.S. industry's access to such markets and projecting American labor and environmental protection values.

Returning to the title of the hearing – assessing controls on investments and technology relevant to threats involving China – the key to doing so properly is more funding for more people in BIS and the other export control agencies to regularly and aggressively conduct and implement such assessments. In light of broad grants of authority in ECRA and FIRRMA, I do not yet believe more law is needed to do so. The issues and technologies involving China are more complex than ever and the need for multilateral cooperation, which is time intensive, continues to remain extremely important to the controls' effectiveness. I believe that each agency is understaffed when compared to its mission. Among other things, this leads to increased burdens and delays for industry, reduced time needed for internal training, insufficient time to study all the issues; and the inability to keep the regulations current. Failure to keep the regulations current to novel threats does not advance our national security interests and harms our economic security.

A renewed attention to supporting these organizations should include efforts to educate the next generation of export control professionals and to motivate them to join the federal government. Decades of wisdom and collective memory will walk out the door when current senior career staff retire or otherwise leave the government. In addition, I

would advocate that the export control agencies have easier hiring authority, more staff to conduct reviews of open source and intelligence community data, more intel analysts, more licensing officers with advanced technical skills, and more staff with foreign language skills, particularly Chinese. Congress was helpful in substantially increasing our budget when I was at BIS, for which I am grateful, but more is needed.

As with all export control topics, I have a three-minute, a thirty-minute, a three-hour, and a three-day version. So, with this, I'll stop here and be happy to answer whatever questions you have.