United States House Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection

"Perspectives on Reform of the CFIUS Review Process"

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

April 26, 2018

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

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

Although I am now a partner at Akin Gump Strauss Hauer & Feld LLP, the views I express today are my own. I am not advocating for or against any issue or potential changes to legislation on behalf of another. Rather, given my industry and government background, I am primarily here to answer your questions about how CFIUS and the export control system work together and how they could work even better to address

emerging national security issues. As requested, I am also willing to comment on the Foreign Investment Risk Review Modernization Act (FIRRMA) (H.R. 4311), particularly with respect to technology transfer issues. My suggestions, I believe, will be constructive and supportive of the essential national security policy objectives motivating the bill's introduction.

I. A Compliment

Before beginning my substantive comments, I would like to point out that this topic is a welcome example of a non-partisan, good faith, regular order, and spirited public debate over legitimate and genuinely difficult national security and economic security issues. I thus want to compliment Senator Cornyn, Senator Feinstein, Congressman Pittenger, Congressman Heck, and all the other co-sponsors of FIRRMA, the Administration, and this and the other committees of jurisdiction for doing such a good job of working through the issues. No one I know or have heard from objects to the bill's policy objective of enhancing our national security given emerging threats from countries of concern and the evolution of dual-use technologies. Most, however, have suggestions for different or modified ways of achieving those objectives with the least amount of collateral regulatory and economic burdens. Discussing them as we are is part of the usual process of getting to a good result.

II. High Level Summary of What the FIRRMA Debate is About

As Derek Scissors will describe in more detail, the policy motivations for the bill stem from the comprehensive Chinese strategy described in the 2015 “Made-in-China 2025” plan. In sum, China has announced plans to become dominant in emerging technologies of strategic importance through indigenous development and acquisition from companies in the US and allied countries. The stated goal is not to join the ranks of the leading high-technology countries but to replace them as such. As the government witnesses described, this is in the context of the general situation where there are often not material distinctions in China between planned civil and military applications of commercial technology or between private and state-owned enterprises. There is direct and indirect state subsidization for the acquisition of emerging technologies and state support for commercial cyber espionage. Technology transfer requirements are often imposed as a condition for companies to do business in China. There are similar concerns with other countries, but most of the discussion has pertained to China.

Different people can easily agree or disagree with any particular response to these issues by this Administration or the previous Administration. All can agree, however, that no one area of law or policy can provide the complete response. Technology-based cyber defenses against bad actors must continue to be enhanced. Investigation and prosecution of those involved in such espionage and traditional intellectual property theft must continue to be supported. Bilateral efforts to negotiate and motivate changes in behavior may be frustrating, but are necessary. Explaining with evidence these concerns to our allies so that they are motivated to take similar whole-of-government responses in their countries is critical. Thoughtful WTO cases and

trade remedy actions consistent with the rule of law and international norms are warranted. Updated and tailored derivative technology transfer and use clauses in government contracts and follow-on compliance are vital. Multilateral trade agreements that have intellectual property, labor, and environmental protections are a useful in exerting multilateral leverage over countries of concern. In the other direction, and perhaps even more importantly, massive amounts of support and attention must be given to investments in the United States for STEM education, general R&D, and infrastructure improvements so that we maintain our edge.

I am here today, however, to discuss only two of the tools the government can use in response – (i) the FIRRMA proposal to update and expand the jurisdictional scope of CFIUS to address investment-based technology transfer concerns and (ii) creatively enhancing the use of existing export controls to address the same issue. From my perspective and with apologies for over-generalizing, there are basically two non-partisan camps in this part of the FIRRMA discussion. Both are reasonable and acting in good faith.

On one side are those who say that CFIUS needs to have significantly expanded jurisdiction over outbound and inbound investments in order to be able to review massively more transactions to determine if they might result in the contribution of technologies of concern, particularly in their earliest stages, and that are otherwise the target of strategic acquisition. Broader jurisdictional authority is needed because technology evolves quicker than regulations or laws can be updated. Transactions are more creative than the government can quickly understand. Given that we are dealing with what are, by definition, novel emerging technologies, the government does not

know what it does not know. One must consider national security threats created by such investment over decades rather than with respect to individual transactions. Thus, the government should have the authority to (i) metaphorically look into most investment boxes going in and out of the country to see if they contain technology, particularly early stage technology, implicating an area of concern and (ii) be able to block or mitigate the transfer given the long-term national security threats. If the technology is not of concern to the destination, then the government will let the transaction go forward.

On the other side are those who believe that before the government uses its extraordinary authority to alter the free flow of civilian commerce, it should do the hard work of identifying the specific technologies of concern and then regulate such technologies, at whatever stage of their development, to the specific end uses, end users, and destinations of concern. Without such tailoring, there is a greater harm to the U.S. industrial base caused by the additional regulatory burdens, approval delays, and investment uncertainties. That is, given a choice between investing or partnering with a U.S. company that will involve such baggage, foreign parties will often choose to invest or partner with companies in allied countries that do not impose such burdens. Some U.S.-based multi-nationals will choose to engage in development efforts outside the United States where the regulatory burdens are lower. Moreover, without such tailoring, the U.S. government's finite resources are burdened by the need to review benign transactions submitted by risk-averse companies when the government should be focusing its resources on the transactions of concern. Finally, the U.S. government already has an entire export control system that can better address concerns in FIRRMA regarding the contribution or other release of technologies of concern. This

side does not deny the national security concern, but rather wants to have it addressed more directly.

The essence of this debate is not new to me. It was inherent in the entire Export Control Reform effort.[1] There was and remains a constant tension in the export control system and regulatory systems in general between controls that are broad and general versus those that are tailored and specific. The former have the virtue of being simpler, but they impose unnecessary controls over less sensitive items and transactions. The latter have the virtue of imposing fewer regulatory burdens, but are harder to craft, are more complex, and require regulatory updates. Based on my experience as a government policy maker, it is generally the case that the more tailored controls that are regularly updated to reflect new information, although harder to create, address the threats more directly and thus with fewer collateral harms. Our experience with the imposition of broad controls on the commercial satellite and spacecraft industry, and then their later tailoring to address the negative impacts of over-controls, are a good example of this point, which I would be happy to discuss separately if you would like.

III. Questions to Ask When Considering Changes to CFIUS

The first question to ask with any contemplated piece of legislation or regulation is "what is the problem to be solved?" As discussed, there are many related China investment and technology transfer issues where the solution to each might be slightly different. Thus, when considering changes to the statutory authority for CFIUS with respect to the issues at hand, I would suggest you ask the following questions:

[1] https://www.bis.doc.gov/index.php/about-bis/newsroom/speeches/speeches-2015/1164-remarks-of-assistant-secretary-kevin-j-wolf-at-the-2016-update-conference

(i) Does the statutory authority already exist to address the issue through a regulatory or process change?

(ii) Would action and related enforcement in another area of law -- such as trade remedies, government contracts, export controls, or intellectual property -- address the issue more directly and without collateral consequences for foreign investments of less concern that we welcome?

(iii) Does the solution lie in providing more resources to the CFIUS agencies to, for example, identify more non-notified transactions that CFIUS should review, monitor more mitigation agreements, or process more cases more quickly with a deeper review?

If the answer to any of these questions with respect to investment-related concerns is "no," then that is the sweet spot for consideration of change to CFIUS legislation.

Without commenting on the merits of any particular change, it is nonetheless vital to weigh the costs of each change. For example, if there is even a small expansion in the scope of CFIUS's review authority, then some companies may be less willing to invest in the United States with the actual *or perceived* extra burden and time involved in closing a transaction, particularly if there is not a significant expansion in CFIUS staff and aggressive compliance with deadlines. With every expansion in scope, there will be a corresponding and exponential expansion in burdens and costs generally. More regulations lead to more words, which lead to more analyses of those words in novel fact patterns, leading to more filings, more reviews, more mitigation agreements, and on and on. Also, if legislation becomes too prescriptive, then it may limit the ability of the Administration and staff to resolve novel national security issues in a creative way. Above all, and regardless of whether national security concerns warrant more or fewer controls, the key question to ask with any change is whether it will create more or less certainty. Even without substantive changes, beneficial investment and international trade are harmed by uncertainties in scope, jurisdiction, timeliness, likely outcome, and

possible enforcement.

The questions I have been answering as part of the public debate over FIRRMA pertain to whether and how the export control system can address the technology transfer-related concerns. The short is answer is that it, with new resources, creative thinking, and a whole-of-government approach, can and should handle the concerns and could do so better than CFIUS could. Indeed, the very reason for the existence of the export control system is to handle such issues. Moreover, why create within CFIUS a new technology transfer regime when one already exists elsewhere within the government, albeit with the need for enhancement? To the extent the investment issue does not pertain to technology transfers, then the export control system is not the solution. Before I get in to the details of these issues, I want to summarize the importance of foreign direct investment and the basics of CFIUS.

IV. Importance of Foreign Direct Investment

Foreign Direct Investment (FDI) is vital to economic growth and job creation in the United States. Assistant Secretary Tarbert and others have described well the statistics regarding the millions of US workers employed by affiliates of foreign companies, the billions of dollars foreign companies invest in America, and how FDI fuels growth for US companies. It was in recognition of these and the other benefits of the free flow of capital in open and competitive markets that Presidents Obama, Bush, Clinton, Bush, and Reagan explicitly reaffirmed the United States' open investment policy and took steps to ensure that we remain the destination of choice for foreign investment. The United States has, in fact, been the destination of choice for FDI

because of such policies, our rule of law, our economy, and our workforce. Competition to attract FDI, however, has never been stronger and companies have many more options around the world than they once did. Therefore, it is vital to our economic security and prosperity that we continue to take actions to make the United States attractive for investment, including modernizing the CFIUS process.

V. CFIUS

The United States, of course, is obligated to protect its national security. We never want to be in a fair fight, and aggressively enforced and properly staffed technology transfer, investment, and other controls are a critical part of maintaining that advantage. Former Assistant Secretary Clay Lowrey, one of the authors of the current CFIUS regulations, other witnesses, and CFIUS staff[2] have well described the evolution and current operations of CFIUS. In sum, the statute authorizing CFIUS gives it jurisdiction over foreign investments into U.S. businesses to identify and address national security concerns. This statutory focus reinforces our long-standing commitment to welcoming investment that does not create unresolvable national security concerns.

By law and in my experience on CFIUS, the Committee does not consider industrial policy or political concerns when reviewing foreign investments. Basically, we would ask ourselves three questions with respect to each transaction. First, is it a "covered transaction?" That is, is it within the scope of CFUIS jurisdiction because it

[2] *See* Committee on Foreign Investment in the United States, 2015 Annual Report to Congress. https://www.treasury.gov/resource-center/international/foreign-investment/Documents/Unclassified%20CFIUS%20Annual%20Report%20-%20(report%20period%20CY%202015).pdf

could give a foreign person the ability, directly or indirectly, formally or informally, to control or affect the activities of a U.S. business? Second, does the transaction present a national security concern? The Intelligence Community is the primary lead for advising whether the acquirer and related parties pose a national security concern. The CFIUS agencies take the primary lead in analyzing whether the national security would be made more vulnerable by the acquisition. Although there is not a binding definition of national security and I will not speak about particular cases, common types of questions we would ask ourselves to get to the answer included:

(i) Are there co-location issues? For example, is the investment in a business near a military facility?

(ii) Would it create espionage risks or cybersecurity vulnerabilities?

(iii) Could it reduce the benefit of certain U.S. Government technology investments?

(iv) Would it reveal personally identifying information that, if exploited, would be harmful to our interests?

(v) Would it create security of supply issues for the Defense Department or other government agencies?

(vi) Would it implicate national security-focused law enforcement equities or activities?

(vii) Would it create vulnerabilities for critical infrastructure, such as with the telecommunications or power grids?

(viii) Is it from a country with a record of nonproliferation or other national security concerns, or that otherwise has a history of taking or intending to take actions contrary to our national security?

(xix) Would it allow technology of concern to be released to foreign persons of concern? For example, was a country of concern seeking to acquire specific technology that, if acquired, could reasonably be used to enhance its military or intelligence capabilities?

Such questions were not asked in isolation. Rather, we would analyze together whether

the combination of any identified threats with a vulnerability would risk impairing our national security. Each of these topics warrants its own, separate analysis and commentary when considering possible changes to CFIUS. The third question we would ask is whether a threat was resolvable by another area of law or through mitigation, *i.e*., through altering the terms of the transaction. The CFIUS agency representatives lead this discussion and contribute their particular expertise and equity to the analysis. If there were an unresolved national security threat, then we would recommend to the President that he block the transaction.

In my experience, the existing CFIUS structure, authorities, and internal procedures generally allowed for the resolution of these issues quite well. The Treasury Department was an excellent honest broker and facilitated consensus conclusions – often after lengthy interagency discussion and always with the terrific support from the intelligence community. The agencies were always respectful of the need for a whole-of-government decision that accounted for the particular equities and expertise of the other agencies. The career staff were and remain talented, dedicated public servants. This last point is key. Given the increase in filings and the increase in more complex cases, the staff was stretched thin when I was there, and I know they are even more stretched now. They need help. They need more resources, particularly aimed at those involved in monitoring mitigation agreements and studying non-notified transactions. I make this polite suggestion not only for their benefit but also for the sake of our national security. I also make the suggestion so that the U.S. remains known as a country that welcomes foreign direct investment with the minimum necessary and quickest possible safe-harbor review burden.

VI. Need for Modernization

FIRRMA's proponents have identified legitimate national security issues the U.S. Government needs to address. The bill contains a number of significant improvements that, if it became law, would improve CFIUS's ability to enhance our national security. Subject to a little wordsmithing by staff and practitioners, examples include:

(i) Enabling CFIUS to review certain real estate transactions unrelated to an investment in a U.S. business if near a military facility.

(ii) Requiring the submission of a declaration if the investment involves significant foreign government interests.

(iii) Expanding the list of national security factors CFIUS may consider when reviewing transactions.

(iv) Improving the monitoring of, and compliance with, mitigation agreements.

(v) Ensuring sufficient funds for additional CFIUS staff at Treasury and its other member agencies.

(vi) Encouraging the Administration to share information with our allies and to work with them on their foreign investment screening and export control regimes.

In particular, I applaud the FIRRMA sponsors' efforts to bring attention to the need to identify and control to countries and end users of concern emerging critical technologies that are not now controlled for release under the export control system to foreign persons but, after an interagency review and public notice and comment process, should be.

VII. Commentary on the new Outbound and Inbound Investment Provisions

Since this is a legislative hearing, I will, as requested, provide my commentary on the bill as introduced. I know, however, that there are significant draft, informal amendments being discussed by the bill's sponsors, the Administration, and the various committees of jurisdiction. Although I will not know with certainty until there is a final formal proposed mark to the bill, I believe that most of my suggestions and comments are consistent with what may be the Administration's view. My two primary comments pertain to the outbound and inbound investment provisions, and my suggestion to use the export control system to identify and control the emerging critical technologies of concern motivating the two provisions.

A. Outbound Investment Provision – Section 3(a)(5)(B)(v)

This provision would expand the definition of "covered transaction" to include "[t]he contribution (other than through an ordinary customer relationship) by a United States critical technology company of both intellectual property and associated support to a foreign person through any type of arrangement, such as a joint venture, subject to regulations prescribed under subparagraph (C)." The bill defines "United States critical technology company" as any "United States business that produces, trades in, designs, tests, manufactures, services, or develops one or more critical technologies, or a subset of such technologies, as defined by regulations prescribed by the Committee."

The provision does not require that the arrangement at issue have anything to do with the contribution or release of critical technology to a foreign person for it to be a transaction subject to CFIUS jurisdiction. Rather, it only requires that some part of the company "trades in," "services," "develops," "produces," etc. "critical technology."

Moreover, the term “critical technology” is defined in the bill to include (i) any technology on any export control list, which includes many widely available commercial and dual-use technologies on the Commerce Control List, and (ii) also any “emerging critical technology” that is not listed on any export control or other list. Virtually all technology companies contribute both intellectual property and associated support to a foreign person in the normal course of business. Thus, far more companies and daily transactions would be within the scope of this provision than it may seem upon first reading.

Such a broad jurisdictional scope would discourage many foreign parties from wanting to enter into transactions with U.S. companies because it would impose U.S. jurisdiction over transactions that, by definition, would not involve the release of technology of concern. The burden and uncertainty would be magnified by the absence of a list of, or even a process to create a list, of emerging technologies the government might deem to be critical. Thus, foreign and U.S. parties would not know whether any particular U.S. company involved with such unlisted technology might be declared to be a “critical technology company.” Foreign companies would often choose not to enter into transactions where there would be even a low risk that the U.S. government might exercise its non-reviewable extraterritorial jurisdiction to alter the transaction. Others would avoid transactions with U.S. companies where there would be a delay as a result of a regulatory filing not required by other countries. Thus, they would often choose to conduct the same venture with a non-U.S. company for the sake of speed and certainty.

Companies proceeding with a transaction that would want to eliminate any possibility, even for seemingly benign covered transactions, that the U.S. government

might later alter the transaction would play it safe and file with CFIUS. This would, by definition, impose unnecessary regulatory burdens and delays on such companies and would significantly add to the CFIUS workload. This could harm the committee's ability to focus its finite resources on the transactions that could potentially involve national security issues.

Finally, the provision as introduced would exempt from its scope the contribution of unlisted emerging critical technology to a foreign person if it occurred during an "ordinary business relationship." This exclusion would thus permit the release to a foreign person of exactly the same emerging critical technology if it occurred during a direct sale but would control the same contribution if done during a joint venture. If the technology is so sensitive that it warrants the U.S. government's having the jurisdiction to alter or block a venture, it warrants being controlled for release to foreign persons of concern regardless of the nature of the underlying transaction.

B. New Inbound Investment Provision – Section 3(a)(5)(B)(iii)

CFIUS already has jurisdiction over any "transaction, which irrespective of the actual arrangements for control provided for in the terms of the transaction, results or **could result** in control of a U.S. business by a foreign person." 31 C.F.R. § 800.301(a). (emphasis supplied). "Control" is defined as meaning "the power, direct **or indirect, whether or not exercised,** through the ownership of a majority or a dominant minority of the total outstanding voting interest in an entity, board representation, proxy voting, a special share, contractual arrangements, formal **or informal arrangements** to act in concert, **or other means,** to determine, direct, or decide important matters affecting an entity; in particular, but without limitation, to determine, direct, take, reach, or cause

decisions regarding [a list of matters], **or any other similarly important matters affecting an entity**. . . .” Id. § 800.204(a). (emphasis supplied).

FIRRMA would add to the list of covered transactions those that include any “other investment (other than passive investment) by a foreign person in any United States critical technology company or United States critical infrastructure company, subject to regulations prescribed under subparagraph (C).” With this provision, CFIUS jurisdiction would apply to non-passive investments that, by definition, *could not* result in control over a U.S. business, directly or indirectly, formally or informally. Moreover, it would apply to investments at any level into a company, including affiliates such as subsidiaries, that meet the broad definition of “critical technology company” even if the investment is completely unrelated to and would not or could not result in the transfer of emerging critical technology of concern to a foreign person.

I would suggest amending slightly the provision so that it is limited to transactions between unaffiliated entities that would or could result in the release or contribution of critical technology to a foreign person from a country of concern by a U.S. business. The policy motivation behind the provision is essentially the same as paragraph (B)(v), which is to have jurisdiction over transactions that might involve the release of such technology to foreign persons of concern. Thus, its scope should be tied directly to the policy it is designed to achieve and there should be a process requiring the government to identify such technologies for the reasons set forth above. Otherwise, it would impose jurisdiction over transactions that, by definition, would not or could not involve the contribution of critical technology. Also, companies involved in unlisted technologies would not know if foreign investments in them are covered. This would create

unnecessary clouds over foreign investment, regulatory burdens, delays, and unnecessary work for CFIUS.

In addition, I do not believe that the bill's sponsors have identified concerns about inbound intra-company transactions, such as a parent company's investing further in its U.S. subsidiary to do additional research. Thus, I would suggest inserting an exemption for transactions among affiliates or between foreign parents and subsidiaries – *i.e.,* between companies with a common ultimate owner.

VIII. A Technology Transfer Control System Already Exists

The apparent underlying policy motivations for the new outbound and inbound investment provisions is a concern that, as a result of transactions in or by a "critical technology company," listed or unlisted technologies of concern, particularly early stage technologies of strategic interest, could be released to a foreign person from a country of concern without the U.S. government's ability to review and potentially control the release of such technologies. This is a worthy concern. However, the U.S. government already has a system with broad statutory authority to identify and regulate the release of technologies of concern -- at any stage of their development -- to foreign persons. It is the export control system. Export controls are the rules that govern

(i) the export, reexport, and transfer

(ii) by U.S. and foreign persons

(iii) of commodities, information/technology, software, and services

(iv) to destinations, end users, and end uses

(v) to accomplish various national security and foreign policy objectives.

In connection with a recent House Foreign Affairs Committee hearing entitled "Modernizing Export Controls: Protecting Cutting-Edge Technology and U.S. National Security," I described the U.S. dual-use export control system in some detail.[3] In sum, the Department of Commerce's Bureau of Industry and Security (BIS) administers the Export Administration Regulations (EAR).[4] These regulations govern the items that warrant control but that are not regulated by another part of the U.S. Government. In essence, they describe on the Commerce Control List (CCL) the commercial, dual-use, and less sensitive military items that warrant control for national security, foreign policy, and other reasons. "Dual-use" items – *i.e.,* commodities, software, and technology – are those that have both benign commercial applications as well as applications of concern. In essence, the EAR controls technology that is required for the development, production, or use of an item. "Development" includes all stages prior to serial production. The controls in the EAR can be as broad or as narrow as the national security concern warrants. The heart of the technology transfer part of the FIRRMA debate is whether there are additional dual-use technologies – *i.e*., emerging critical technologies – that are not now controlled but that should be in light of the evolving threats that I described earlier.

Identifying and controlling technologies is not the only tool the EAR has to address national security concerns. It also has the authority to impose controls on all exports and reexports of items subject to US jurisdiction to specific foreign persons or companies of concern. It also has the authority to impose controls on specific end uses

[3] https://docs.house.gov/meetings/FA/FA00/20180314/107997/HHRG-115-FA00-Wstate-WolfK-20180314.pdf

[4] https://www.bis.doc.gov/index.php/about-bis/mission-statement

of items even if the underlying technology is widely available. Controls can be unilateral as needed, but the better controls are those that are multilateral so that our allies are working with us to achieve the same policy objectives.

BIS is responsible for leading interagency efforts to identify and control such technologies. As described in my HFAC testimony in more detail, the Departments of Defense, State, and Energy are the primary participants in this effort, but BIS takes input from all parts of the government with equities and expertise in the topic at hand. The lists are thus regularly evolving to take into account new national security concerns and new facts. After a technology or other item is identified, the controls on its transfer can be tailored in the regulations to apply to the whole world or to specific destinations, end uses, and end users to address specific concerns. The control choice is a function of a national security and foreign policy judgment to be made on a technology-by-technology basis and regardless of the existence or nature of any underlying commercial transaction. That is, export controls apply to exports or other releases of technology regardless of, for example, whether the exporter is owned or controlled by a foreign parent, the transaction is a sale or a joint venture, or the release is tangible or intangible.

In my experience, the existing export control system works well. BIS and its sister agencies are full of talented, dedicated, and motivated public officials. Given the (legitimate) increase in attention to analyzing emerging technologies, at whatever stage of their development, more resources are needed for them to do this work on top of their regular efforts. In my opinion, the answer to the inbound and outbound FIRRMA provision process issues I described earlier is essentially in section 109 of the Export

Control Reform Act of 2018 (H.R. 5040) introduced by Congressmen Royce and Engel.

In sum, it requires the Administration to:

1. enhance the existing export control system with a regular, well-funded interagency effort to get from national security, intelligence, and industry experts information and predictions regarding uncontrolled technologies that are (a) emerging and critical to maintaining our military and intelligence advantages, and (b) the subject of acquisition efforts by countries of concern that, if so acquired, would be harmful to our interests;

2. absent an emergency need to publish unilateral controls immediately, publish proposed amendments to the export control rules for public comment to make sure the descriptions of such technologies are clear and do not contain unintended collateral consequences unrelated to or that would harm our national security;

3. publish final export controls tailored to the destinations, end uses, and end users of concern, regardless of the nature of the underlying transaction;

4. educate the U.S. and foreign public, and our allies, on the controls and the reasons for why they are needed;

5. work with the relevant export control regimes to develop common, multilateral controls over the new technologies – *i.e*., so that the technologies are controlled by allies as well as when sent from the United States;

6. provide healthy resources and tools to the law enforcement agencies so that they can properly investigate and prosecute violations of the new and the old controls; and

7. institutionalize a system to regularly review, revise, and update the controls so that they do not become outdated as threats evolve and more information is gathered.

My standard joke is that I have a three-minute, thirty-minute, three-hour, and three-day version of every export control topic. So, I will stop here. Thank you again for spending the time to think through this complex and important national security issue. I am happy to answer whatever questions you have.