United States House Committee on Foreign Affairs
"Modernizing Export Controls: Protecting Cutting-Edge Technology and U.S. National Security"

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)

March 14, 2018

Chairman Royce, Ranking Member Engel, and other distinguished members of the committee. Thank you for convening this hearing and for inviting me to testify on this important national security topic. It is a pleasure being back before the committee.

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, I am here to answer your questions about how the export control system works, how it should be modernized to protect cutting-edge technologies that warrant controls for national security reasons, and any other related policy topic you would like to discuss.

What are Export Controls?

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.

That is my entire professional life in one sentence. Although it appears deceptively simple, each export control decision requires complex, multivariate policy and legal analyses involving statutes, regulations, international commitments, intelligence and law

enforcement equities, threat assessments, industrial base implications, license administration, budgets/resources, corporate compliance considerations, foreign availability, interagency dynamics, congressional concerns, and multilateral and bilateral foreign policy issues. The technologies are often complex, 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. Technologies that were once sensitive become ubiquitous, such as the GPS technology in our cell phones. Generally non-sensitive commercial technologies can 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. But 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.

Controls Should be Tailored to Address the National Security Concern

National security concerns are, of course, paramount and should be the basis for any final decisions. The United States never wants to be in a fair fight. The appropriate, aggressively enforced, clearly written, and *well-funded* export and related controls are a critical part of maintaining that advantage. I have never subscribed to the view that export controls should "balance" national security concerns with economic concerns. National security concerns are not to be traded off for something else in a particular transaction or in trade deals. Rather, they should be properly calibrated, tailored controls to avoid collateral economic costs, unnecessary regulatory burdens, and misallocation of federal resources. Excessive controls harm the U.S. defense industrial base, which results in harm to our national security. Lax, out of date, or poorly enforced controls have the same effect.

Export controls are *not* the solution to all policy concerns. They are also not tools for industrial policy. They should be used to their fullest possible extent, however, when a national security 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, 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.

The "Four Singles" Idea

Many parts of the U.S. Government regulate the export of items for various reasons. As discussed many times during my government tenure, my view is that the administration of the export control system should be consolidated under one roof, under one set of regulations, with one information technology and online licensing system, and one export enforcement coordinating authority. Such a system would accomplish our national security and foreign policy objectives more efficiently and with dramatically fewer regulatory burdens. It should, of course, draw upon the expertise and equities of all relevant federal agencies and industry experts when deciding what to control where

and how, but why impose on industry and the government different rules, different words, different forms, and different procedures to accomplish the same goal? That was not to be, however, and will have to wait for another day to be considered again.

The Bureau of Industry and Security (BIS) and the Export Administration Regulations (EAR)

For purposes of today's hearing, though, the system at issue is the one managed by the Department of Commerce's Bureau of Industry and Security (BIS), which administers the Export Administration Regulations (EAR). 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.

BIS and the EAR also play an important role in furthering and complementing the foreign-policy based sanctions and embargoes administered by the Treasury Department. The EAR also contains Short Supply control authority and anti-boycott regulations. These issues, however, are not the topic of today's hearing. Also not subject to today's hearing are the International Traffic in Arms Regulations (ITAR), administered by the State Department. They regulate sensitive military items under the authority of the Arms Export Control Act.

The authority for the relevant parts of the EAR rests upon a 2001 Executive Order and annual presidential notices continuing the emergency need for the regulations under the authority of the International Emergency Economic Powers Act (IEEPA). As properly stated by the Chairman and Ranking Member, The Export Control Reform Act of 2018 (H.R. 5040) is the first real push to establish *permanent* authority for the EAR since the Cold War-era Export Administration Act (EAA) of 1979 expired in 2001. My personal view is that the bill's statement of policy in section 102 for this part of the export control system is perfect.[1] I applaud the members for addressing this issue. Many of the threats and technologies are very different now than they were in 1979 and the issue warrants evaluation more frequently than every 40 years.

What are Dual-Use Technologies and Why Regulate Them?

This reality gets right to the heart of the title of this hearing – how are cutting-edge dual-use technologies that warrant control identified and regulated? "Dual-use" items – *i.e.*, commodities, software, and technology – are those that have both benign commercial applications as well as applications of concern, such as those pertaining to military applications and weapons of mass destruction. The machine tool that can be used to make a commercial aircraft part could also be used to make a missile skin. The

[1] I did, however, notice what appear to be unintentional drafting errors in the bill with respect to, for example, the definition of "U.S. Person" and the scope of foreign items that could be subject to the jurisdiction of the regulations. I will suggest technical fixes to staff after the hearing.

microelectronic circuit that is important for a cellular phone network might be critical to a military radar.

As this core definition indicates, not everything that is cutting edge or emerging warrants control. In fact, most such technologies clearly do not. So, a government must work backwards and identify the threats first. What are the technologies and other items, real and prospective, that will maintain the United States' military and intelligence advantages over other countries and adversaries? What are the technologies and items that others seek or are likely to seek to eliminate that advantage? What are the foreign policy considerations, including human rights concerns, that warrant imposing controls? In short, the answer to the question is that the export control system gets such input and information from multiple sources and Commerce's BIS coordinates its implementation in to a regulatory, licensing, education, and enforcement system.

Which Parts of the Government Constitute the Dual-Use Export Control System?

The Defense Department, including its services, labs, and many experts, has a significant, if not primary, responsibility for identifying such technologies. The **Defense Technology Security Administration (DTSA)** is DoD's point of contact for the export control system and makes DoD's recommendations pertaining to foreign access to U.S. technology and other items. The National Security Agency's Industry and Academic Engagement group provides technical support to BIS regarding controls over the export of encryption.

The State Department's **Bureau of International Security and Nonproliferation (ISN)** leads the department's efforts to prevent the spread of WMD and their delivery systems. It is the export control system's point of contact for the State Department's expertise in these areas and the department's foreign policy assessments of transactions. ISN is also the leader of the interagency efforts to coordinate and revise U.S. export controls with those of our multilateral export control regime partners in The Wassenaar Arrangement (conventional arms and dual-use items), the Nuclear Suppliers Group, the Australia Group (chemical and biological weapons), and the Missile Technology Control Regime. Through such efforts, the United States is able to propose and get coordinated controls among allies and others on technologies and other items of common concern. It also benefits through this system from the expertise and insights of our regime allies in identifying items of concern, including emerging technologies.

The **National Nuclear Security Administration (NNSA)** coordinates the input and expertise of the Department of Energy, primarily pertaining to matters involving nuclear science, into the dual-use export control system.

The Commerce Department's **Bureau of Industry and Security (BIS)** is responsible for reducing all such efforts, input, and expertise into the content and administration of the EAR. It is the point of the contact for the Commerce Department's views on export controls and responsible for running an efficient, coherent, reliable, enforceable, and predictable export control system, including resolving competing agency views or policy

objectives. Its mission statement (which includes more than just export control issues) is at: https://www.bis.doc.gov/index.php/about-bis/mission-statement. Its licensing officers and other officials are experts in their areas of responsibility and generally have engineering, scientific, military, intelligence, or foreign policy backgrounds. Export control rules are inherently complex. To ensure that they achieve their objectives, and to reduce unnecessary regulatory burdens (particularly on small- and medium-sized businesses), BIS's mission includes the provision of a substantial amount of industry education and outreach. BIS also has its own enforcement authorities and an Office of Export Enforcement (OEE) with special agents focused on investigating and, in close coordination with the Department of Justice, the Federal Bureau of Investigation, and the Department of Homeland Security, enforcing the EAR. OEE is also BIS's point of contact with the intelligence community and provides input on licensing determinations.

Thus, DTSA, ISN, NNSA, and BIS are the responsible reviewing agencies for dual-use export control determinations, including decisions to list, revise, or remove a control, as well as case-by-case decisions on individual applications seeking a license to engage in a controlled activity. Although not part of the dual-use licensing system, BIS coordinates with the State Department's Directorate of Defense Trade Controls (DDTC) to prevent jurisdictional overlap with the sensitive military items subject to its control. In addition, BIS draws upon the expertise of other parts of the U.S. Government as needed, such as the Department of Homeland Security, National Institutes of Health, and the National Aeronautics and Space Administration.

Finally, BIS has technical advisory committees of industry experts in the technology areas for which BIS is responsible. They provide industry input into new technologies and new applications of old technologies to help BIS further its mission. The members have security clearances and have the authority to meet in both public and non-public sessions. They are a vital tool for BIS to use when identifying emerging technologies of concern.

The Export Control Reform (ECR) Effort

During the Obama Administration, all this expertise was applied in a massive seven-year effort involving hundreds of experts and affecting tens of thousands of items to review and substantially update the lists of military items. The goal was to identify and distinguish between those items that provide the United States with a critical or significant military advantage, and those that are less sensitive. If an item was identified as being militarily critical, important, or unique, it was listed on either the State Department's U.S. Munitions List or the Commerce Department's list of new military controls, and controlled according to its sensitivity.

Our national security was enhanced as a result of this effort because it (i) helped to increase military interoperability with our NATO and other close allies, (ii) helped the defense and space industrial base by reducing the incentives for allies to design out or avoid U.S.-origin content, (iii) made the rules more reliable and predictable, and (iv) allowed the government to focus its resources more on transactions, end uses, end

users, and destinations of concern. The background to this fourth point is that too many government resources were devoted to reviewing and approving transactions of less sensitive items in the allied supply chain (that were never denied), when we should have been focusing more of our attention on the more sensitive items and trade involving the countries, end uses, end users of more concern.

Emerging and other items of concern identified as a result of this effort were evaluated and led to amendments of dual-use controls and changes to the international control lists. Our experience with microwave monolithic integrated circuits (MMICs) is a perfect example of this process. MMICs have long been important parts of military radar systems. As a result of the reform effort, the government learned more about their commercial technology evolution and large number of non-military applications, such as with respect to commercial telecommunications systems. This work led to substantial revisions of the military and dual-use controls, both in the United States and in the regimes, over such items.

So that the revised military controls stayed current, we set in motion a process requiring each of the categories to be evaluated every two years or so to account for evolutions in technology, commercialization, and new threats. The system would also be user friendly in that it would correct mistakes and, based on the past experience, find ways of describing the controls more clearly. The Trump Administration has continued this effort and is now, for example, beginning the process of getting industry and government input on how controls on military electronics and other items should be updated.

This is not to say that we did not review and revise the dual-use controls during the reform effort. To the contrary, there were substantial revisions to these controls over the years, primarily as a part of the regular efforts to revise and update the multilateral export control lists. It is, however, a fair comment that we devoted extra efforts to identifying and describing better controls on military items and only traditional efforts to identifying and describing new commercial technologies that could be of concern. We often said that we wanted to do a top-to-bottom scrub of the dual-use controls at the same level of intensity we were doing for military controls, but military priorities and resource constraints did not permit it.

Renewed Attention to Unlisted Commercial Emerging Technologies of Possible Concern

It is for this reason that I compliment Congressmen Royce and Engel for highlighting the need for such an effort in their export control bill. I also compliment Senator Cornyn, Senator Feinstein, Congressman Pittenger, and all the other co-sponsors of the Foreign Investment Risk Review Modernization Act (FIRRMA), and the Administration, for highlighting and creating a robust public debate over the best ways to identify and regulate the transfer of emerging critical technologies of concern that are not yet controlled but that should be.

These legislative discussions have clearly given a kick to the system to be sure that it does not get too comfortable with evaluating just the traditional WMD, military, and dual-use technologies of concern that it knows about. The system should put in extra outside-the-box efforts with experts not normally part of the export control system to study emerging technologies in commercial sectors that it may not ordinarily come across. I do not now have recommendations for which specific emerging technologies are not now controlled but should be, but I am confident that a regular interagency process focused on this topic that draws upon all available experts will get to the best answer.

How long it will take to get to such answers is a function of the resources put into the effort and the creativity of those involved. Even with massive attention and resources, however, the task will not be an easy one. The several specific emerging technologies, such as additive manufacturing and driverless vehicle technology, that we studied for possible controls during my time proved to be particularly difficult in revealing which parts or subsets warranted controls to address an actual or possible treat. Clamping down too hard on an emerging technology will drive research and development in the areas offshore, which hurts our national security. Not controlling it enough can result in the shrinking of the military and intelligence advantages we have that I discussed earlier.

Current Authorities to Control Unlisted Emerging Technologies of Concern

That we did not have a regular, separate research effort focused on emerging commercial technologies does not mean we were not thinking about the issue. Indeed, we were so concerned about the possibility of inadvertently missing something during the military list review effort or later discovering a new technology of concern that we wanted to make sure we had the authority to regulate it quickly and without hassle. This is why I and my colleagues at BIS created a novel tool in the EAR to allow us to quickly and unilaterally control emerging and other unlisted technologies that warranted control, so long as the technology was eventually submitted to the relevant regimes to be controlled multilaterally.[2] This is referred to as the "0Y521" series of controls in the EAR, which mirrors similar authority in U.S. Munitions List Category XXI in the State Department's International Traffic in Arms Regulations.[3]

Thus, if BIS or any other agency identified a previously uncontrolled technology that warranted control because its uncontrolled release could harm our national security or foreign policy interests, BIS could impose controls on its export, reexport, and transfer immediately without needing to wait for a public notice and comment process or getting consensus among the multilateral regime partners. This is a short-term fix because the best controls are those that benefit from industry input (to ensure that the descriptions are clear and without unintended consequences) and that are controlled similarly by the allies (to further the common objectives of the controls and to level the playing field). Nonetheless, the authority exists today to control immediately emerging technologies of

[2] *See* 77 Fed. Reg. 22191 (Apr. 13, 2012).
[3] *See* 22 C.F.R. § 121.1.

concern at any stage of their development once someone in the government identifies the technology in a way that can be reduced to regulatory control text and can provide the required national security or foreign policy justification for the control.

A key element to this control (and ideally, all controls) is that the scope is clear. Vague descriptions of what is controlled that leave exporters and foreign parties uncertain about what is within the control harm both compliance objectives and impose unnecessary economic harms. For regulations to work, all parties involved must know what and is not captured by a control. Uncertainty discourages otherwise legitimate exports and imposes compliance costs on companies that need to analyze the transaction longer than necessary.

The EAR Has Many Tools Available for Addressing National Security and Foreign Policy Concerns

Not all concerns pertaining to technology are best addressed through identifying it on a control list for general controls. Sometimes, the technology as such is not the issue, but its application by specific end users is the concern. That is, BIS, through intelligence or other sources, comes across information that a particular end user is going to put otherwise non-sensitive or old technology to a bad end use. The EAR allows for tailored controls to specific end users, such as through the "is informed" process and the Entity List process. This means that BIS can inform particular parties that specific exports are of concern and require authorizations without imposing burdens on all other exports of the same technology. The Entity List process allows BIS to add particular foreign entities to lists that, in the main, result in a prohibition on the export of all items, listed and unlisted, from the United States. This can create economic incentives for the listed entities, which are generally outside United States jurisdiction, to stop engaging in acts contrary to our national security and foreign policy interests. The EAR also imposes controls on otherwise uncontrolled items if they are destined for end uses of concern, such as WMD applications worldwide or military end uses in China or Russia. Finally, the EAR allows for prohibitions on activities of US persons if they are for WMD-related activities, even if items subject to the regulations are not involved.

Thus, the EAR is clearly and deliberately not a "one-size-fits-all" type of regulation, which is its virtue and its vice. It is a virtue because it allows for tailored controls to address the concern at issue without imposing unnecessary regulatory and economic burdens on transactions not of concern. That is, paradoxically, also its vice because, with tailored controls, comes complexity and the need for the government do to the hard work up front of identifying what the threats are and regulate for them thereafter. Controls that regulate everything equally everywhere all the time are safe and easy to create -- and absolutely needed for military crown jewels and inherently critical items -- but, for all other items, impose many collateral burdens that do more harm than good.

The EAR Controls Are Tailored to Different Types of Items

The inherent complexity in the EAR is magnified when considering that its controls include physical items, software, and technology – and the technology controls are further divided primarily among developmental technology, production technology, and use technology. Often the technology is more of a concern than a physical item and developmental technology is of more concern than operational technology. Moreover, the descriptions of technology in the regulations can be as broad or as narrow as the national security or foreign policy concerns warrant. They are generally connected to physical commodities, but do not need to be. They could be based on a technology's technical parameters, end uses, stage of development, or merely just a reference to the name of the technology.

After a technology or other item is identified, the controls on its transfer can be tailored in the regulations to apply to the whole world or to specific destinations, end uses, and end users to address specific concerns. The control choice is a function of a national security and foreign policy judgment to be made on a technology-by-technology basis and regardless of the existence or nature of any underlying commercial transaction. That is, export controls apply to exports or other releases regardless of, for example, whether the exporter is owned or controlled by a foreign parent, the transaction is sale or a joint venture, or the release is tangible or intangible.

Effective, Well-Funded Enforcement is Critical to the Success of the System

The effort to identify emerging and other technologies of concern, describe them in the regulations, and educate the public about them, however, is meaningless unless there is effective enforcement of the controls – and unless law enforcement officials have the tools they need to do their jobs. There are regular interdiction efforts of items destined to an end use or end user of concern. There are on-site audits in the U.S. and abroad that stop illegal acts before they occur. There are undercover efforts and stings. There are tips provided by commercial competitors and allies about likely violations. There is a long list of criminal prosecutions of export control violations to prove these and related points.

The system, however, *like most regulated areas*, largely relies on voluntary compliance motivated by a fear of being subject to painful civil or criminal penalties for non-compliance. It is impossible for the government to review every transfer of technology from or outside the United States and the contents of every box going through a U.S. or foreign port. Most technology transfers are intangible and the tangible volumes are massive and overwhelmingly not items of national security concern. Robust export control law enforcement is thus needed to motivate those on the front lines of exporting from the United States and *reexporting controlled items outside the United States* to develop and maintain comprehensive programs to ensure compliance with the rules, regardless of whether the company is domestic or owned by a foreign entity. I know it may seem counter-intuitive to think that industry should advocate for well-resourced,

level-headed law enforcement, but it is actually critical to keeping the playing field level for those companies that do the hard work to stay compliant.

Given the inherent complexity in the system, it is also critical that there is a core group of enforcement officials specially trained and focused on export control enforcement – and that the public knows they have all the tools and resources they need to do their jobs. Although the full law enforcement resources of the U.S. government are absolutely needed to motivate compliance, the topic is not one to be left exclusively to enforcement officials distracted by other priorities. Law enforcement personnel dedicated to export control compliance are also often better able to work with their foreign counterparts to ensure joint efforts to identify and stop export control violations outside the United States. Such a group, by the way, already exists in BIS's Office of Export Enforcement.

The Existing System Works Well, but Could Benefit from More Resources and Attention to Novel Issues

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. I make this polite suggestion not only for their benefit but also for the sake of our national security.

On every export control issue, I have a three-minute, a thirty-minute, a three-hour, and a three-day version. So, I will stop here with a summary answer to the core question of this hearing, which is how do we control cutting-edge technologies to protect our national security? The answer is in section 109 of your bill, which, in sum, says:

1. enhance the existing export control system with a regular, well-funded interagency effort to get from national security and intelligence experts not normally part of the system information and predictions regarding new technologies that are critical to maintaining our military and intelligence advantages;

2. identify the types of technologies, at whatever stage of their development, that are necessary to maintain such advantages;

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

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

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

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

7. 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

8. institutionalize a system to regularly review, revise, and update the controls so that they do not become outdated.

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.

The Structure of All US Export Control Law

Act: Export, Reexport, or Transfer / Actor: US Person or Foreign Person (people and companies)	Physical Things ("Goods," "Commodities," "Defense Articles")	Information ("Technology," Technical Data")	Software	Services ("defense services" or WMD-related "activities")	Transactions (e.g., agreements or transferring money)
Destinations (Countries or regions, for listed items, or embargoed destinations for all else)					
End-Uses (e.g., WMD end uses regardless of item's classification)					
End-Users (e.g., SDNs or Listed Entities, regardless of item's classification)					