Testimony before the Senate Committee on Banking, Housing, and Urban Affairs
"Export Control Reform Implementation: Outside Perspectives"

Nova J. Daly
Former Deputy Assistant Secretary of Treasury for Investment Security (2006-2009)
Senior Public Policy Advisor, Wiley Rein LLP
July 18, 2019

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

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

I. Provides an assessment of the current implementation and enforcement of ECRA, including related regulations;
II. Describes how the United States may establish controls that address emerging and foundational technologies while preserving domestic innovation;
III. Addresses recent designations of Zhongxing Telecommunications Equipment Corporation ("ZTE"), Huawei Technologies Co. Ltd. ("Huawei"), and other Chinese technology companies;
IV. Discusses whether ECRA-related control structures in the United States will be effective in confronting the challenges raised with respect to China, including the persistent diversion challenges China evokes; and
V. Proposes possible legislative or oversight recommendations regarding the topics covered today.

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

[1] Subtitle B, Part 1, P.L. 115-232
[2] Title XVII, P.L. 115-232

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

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

As Commerce Secretary Wilber Ross recently noted, "[e]conomic security is essential to national security" and safeguarding our technology "is not easy, since the boundaries between civilian and military technologies become ever more narrow as technologies are increasingly omnipresent."[5]

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

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

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

---

[3] P.L No: 115-232

[4] E.O. 13873, "Securing the Information and Communications Technology and Services Supply Chain."

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

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

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

As controls on exports of technology are a key component of the effort to protect sensitive U.S. technology, many sensitive technologies are listed on the Commerce Control List (CCL), often consistent with the lists maintained by the multilateral export control regimes of which the United States is a member. Certain technologies, however, may not yet be listed on the CCL or controlled multilaterally because they are emerging technologies. As such, they have not yet been evaluated for their national security impacts. This advance notice of proposed rulemaking (ANPRM) seeks public comment on criteria for identifying emerging technologies that are essential to U.S. national security, for example because they have potential conventional weapons, intelligence collection, weapons of mass destruction, or terrorist applications or could provide the United States with a qualitative military or intelligence advantage. Comment on this ANPRM will help inform the interagency process to identify and describe such emerging technologies. This interagency process is anticipated to result in proposed rules for new Export Control Classification Numbers (ECCNs) on the CCL.

Commerce does not seek to expand jurisdiction over technologies that are not currently subject to the Export Administration Regulations ("EAR"), such as "fundamental research" described in § 734.8 of the EAR. For purposes of this ANPRM, Commerce does not seek to alter existing controls on technology already specifically described in the CCL. Such controls would generally continue to be addressed through multilateral regimes or interagency reviews.

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

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

BIS has additionally made clear that achieving multilateral controls on these technologies would make the most sense and that the process of identifying and implementing controls on emerging and foundational technologies will be ongoing, consistent with BIS's normal rulemaking approach. Toward that end, it should be noted that as a result of a Wassenaar Plenary in 2018, in May 2019, BIS published a final rule that revises the CCL to implement certain changes made to the Wassenaar Arrangement List of Dual-Use Goods and Technologies maintained and agreed to by governments participating in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ("Wassenaar Arrangement").[8]

[8] This rule added five recently developed or developing technologies (i.e., emerging technologies) that are essential to the national security of the United States to the EAR's CCL, including discrete microwave transistors (a major

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

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

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

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

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

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

Currently, the United States has four multilateral regimes for export controls: the Wassenaar Arrangement; the Australia Group; the Nuclear Suppliers Group; and the Missile Technology Control Regime. Through each of these regimes, countries identify the items to control (i.e., products, software, and technology), but the controls must be implemented in national legislation. More specifically, while countries multilaterally agree on controls of specific items, all countries have divergent licensing policies on their exports, some with stringent policies restricting exports, and some with more relaxed policies. This issue can frustrate the purpose of a multilateral regime because companies facing more stringent policies in certain countries cede global market share of the controlled items to companies in countries with more relaxed policies. The resultant pressure

component of wideband semiconductors), continuity of operation software, post-quantum cryptography, underwater transducers designed to operate as hydrophones, and air-launch platforms.

on countries to protect market share often leads to an underutilization of export control authority. This is not to mention that the controls themselves are not effective when countries have different licensing policies.

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

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

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

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

While at Treasury running the CFIUS process, I saw first-hand the limitations of the voluntary process where actors acquired new and critical technologies outside of CFIUS's purview. Now with ECRA and FIRRMA, we can better safeguard the loss of our critical technologies (including emerging and foundational technologies) to those who would do harm to our economic and

national security. Since my service in government, I have observed an increasing number of transactions involving Chinese parties where the technology at issue could be viewed to present a lower threat, but the actual threat posed by the transaction related to vulnerabilities in the U.S. supply chain. Such vulnerabilities augment the ability of rogue actors to leverage the U.S. supply chain thereby raising national security concerns, including: undercutting direct competitors; eroding the existing U.S. technology of acquired companies; impacting the availability of upstream inputs; and undermining the ability of downstream purchasers and producers to compete.

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

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

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

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

Prior to Huawei's designation, BIS also targeted ZTE. In March 2016, ZTE and several of its affiliates were added to the Entity List for their involvement in a scheme to reexport U.S.-controlled items to Iran. ZTE reached a settlement with BIS in March 2017, paying a total of US$1.19 billion in fines, and was subject to a suspended denial order. Having not complied with certain conditions of that settlement, BIS activated the Denial Order on ZTE in April 2018. The import ban has since been lifted as ZTE agreed to a settlement with BIS with significant conditions,

[9] See, "Washington unnerved by China's 'military-civil fusion," Kathrin Hille, Financial Times, November 8, 2019.
[10] 15 C.F.R. Pt. 744, Supp.4

including a US$1 billion fine. BIS rightfully took a strong stance against ZTE, imposing unprecedented compliance measures as part of the settlement. These actions demonstrate a robust commitment on the part of the Administration to combat technology-related national security issues. Such efforts were necessary and long overdue.

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

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

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

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

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

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

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

V. Possible Legislative or Oversight Recommendations

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

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

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

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

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

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

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