

## **Testimony before the U.S.-China Economic and Security Review Commission**

Hearing on “China’s Pursuit of Defense Technologies: Implications for U.S. and Multilateral Export Control and Investment Screening Regimes”

Panel III: “Policy Tools for the United States and Its Allies and Partners”

Cordell A. Hull

Former Acting Under Secretary of Commerce for Industry and Security (2019-2020)

Visiting Fellow, National Security Institute,

George Mason University Antonin Scalia Law School

April 13, 2023

### **Introduction**

Chairman Bartholomew and Vice Chairman Wong, it is a pleasure to be before the Commission this afternoon. I am delighted to be joined on this panel by Martijn Rasser and Emily Kilcrease, both distinguished experts in their fields.

My testimony today will focus on: (i) how export controls address the People’s Republic of China’s (PRC) military modernization; (ii) the government’s effectiveness in identifying and controlling technology to ensure it is not illicitly transferred to the PRC; (iii) potential steps to streamline the export-control process; (iv) effectiveness of enforcement; (v) government and private-sector coordination; and (vi) policy recommendations for the Commission.

Before providing my remarks, I would like to state that I am testifying to you today in my capacity as a Visiting Fellow at the National Security Institute of George Mason University’s Antonin Scalia Law School. The views expressed in my testimony are personal and do not reflect the views of any organization with which I am affiliated.

While in government, I had the privilege to see export controls and foreign investment from the legislative branch and implementation in the executive branch. While serving as the Acting Under Secretary for Industry and Security at the Department of Commerce, I worked with my interagency colleagues to implement the Export Control Reform Act of 2018 and, to a lesser extent, its companion legislation the Foreign Investment Risk Review and Modernization Act (ECRA and FIRRMA, respectively). Both pieces of legislation were items I worked on when I was the General Counsel of the House Permanent Select Committee on Intelligence.

As is clear from my background, I have a strong view of national security, and in particular the challenges posed by the PRC. My time as under secretary was spent implementing ECRA and FIRRMA to meet the many and varied challenges posed by the PRC.

From China’s increasing assertiveness to disrupt the rules-based international order, to its repression of human rights, to its well-known practice of military-civil fusion (MCF), it is an export-control challenge unlike any this country has faced before.

Adding to the fact that China is our country’s largest trading partner, and our economies are intertwined to an extent never before seen with a foreign adversary, we must remain laser-

focused on ensuring our technology and innovation are not turned against us. But we must do so in a way that does not unnecessarily inhibit research and development that has enabled us to out-innovate much of the world.

It is important to bear in mind that export controls are a time-limited solution and that controls may get less effective each day as technology advances and/or adversaries find work arounds. To be optimally effective, they must account for foreign availability and should be implemented with other actions, such as investment restrictions, but also ensuring we continue to run faster.

We must also recognize that the world is shrinking. No longer can we unilaterally control a wide variety of items and have a preclusive effect on inhibiting our adversaries' abilities to obtain them. Working with allies and partners is essential to ensure that controls we put in place are effective while taking care not to limit progress. Our mantra should be: multi- or plurilateral where we can, unilateral where we must.

Let me be clear: if the call is a close one, national security must always win.

But as the U.S. government moves to create and implement new tools in the export-control arena, it must ensure that it is doing so in a way that does not inhibit innovation, has a clear view of the national security problem it is trying to solve, and uses all sources of information to solve that problem.

### **U.S. export control system's role in China's defense modernization**

The last decade or so has seen a profound shift in the way we consider dual-use export controls related to PRC.<sup>1</sup> The U.S. government, led by the Department of Commerce's Bureau of Industry and Security (BIS), where I served, has led the way in implementing that shift.

While several of the actions listed below represent successes in the U.S. government's efforts to ensure American technology is not being used against our interests, more can and should be done.

#### **Entity List**

Perhaps the most publicly known change is the enhanced use of the Entity List. That list permits BIS to impose a license requirement under the Export Administration Regulations (EAR) for exports to parties on the list when they are "believed to be involved" or risk becoming involved "in activities contrary to the national security or foreign policy interests of the United States."<sup>2</sup> The U.S. government has broadened the use of the list mostly from front companies diverting

---

<sup>1</sup> I use the caveat of "dual use" because shipments of defense articles or services have been largely prohibited to China because of the uprising in Tiananmen Square in 1989. Following the PRC's actions to stifle pro-democracy protestors, Congress amended the Arms Export Control Act and its implementing regulations, the International Traffic in Arms Regulations. 22 U.S.C. § 2778; 22 C.F.R. § 126.1 (listing China as a country subject to a "policy of denial"); *see also* Name Redacted, China: Economic Sanctions, CONG. RES. SERV., R44605, at 6 (2016), <https://bit.ly/3FBX9rL>.

<sup>2</sup> 15 C.F.R. § 744.16.

controlled technology and scientists involved in proliferation activities to large multi-national companies. That use brought about wide-ranging effects on U.S. and allied industry.

The addition of Huawei in 2019,<sup>3</sup> then the largest telecommunications firm in the world, brought the list into the consciousness of many Americans. In the years since, there have more than 100 Huawei-related entities added to the list. BIS also added the Semiconductor Manufacturing International Corporation (SMIC), China's national champion semiconductor fabrication company, due to its support of the PRC's military modernization efforts.<sup>4</sup>

The Entity List's expansion has not been limited to Huawei and SMIC. There have been novel listings related to human rights in the Chinese Communist Party's (CCP) repression of Uyghurs and other members of Muslim minority groups in the Xinjiang Uyghur Autonomous Region (XUAR);<sup>5</sup> malign activities in the South China Sea;<sup>6</sup> and trade-secret theft.<sup>7</sup>

A recent listing further underscores the scope of this shift to ensure the PRC's military is not using our technology and innovation against us or for repression around the world. In March 2023, BIS added three subsidiaries of BGI, f/k/a Beijing Genomics Institute, to the Entity List because the "actions of these entities concerning the collection and analysis of genetic data present a significant risk of diversion to China's military programs."<sup>8</sup>

Showing the utility of the Entity List, BIS recently issued a rule that made it easier to add companies to the list where they or their government fail to cooperate with end-use checks.

---

<sup>3</sup> Addition of Entities to the Entity List, 84 Fed. Reg. 22961 (May 21, 2019) (adding Huawei Technologies Co., Ltd. and more than 60 of its affiliates to the Entity List).

<sup>4</sup> Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities from the Entity List, 85 Fed. Reg. 83416 (Dec. 22, 2020).

<sup>5</sup> Additions to the Entity List; Amendment To Confirm Basis for Adding Certain Entities to the Entity List Includes Foreign Policy Interest of Protection of Human Rights Worldwide, 88 Fed. Reg. 18983 (Mar. 30, 2023); Additions and Revisions to the Entity List and Conforming Removal from the Unverified List, 87 Fed. Reg. 77505 (Dec. 19, 2022); Addition of Certain Entities to the Entity List, Revision of Existing Entry on the Entity List, Removal of Entity from the Unverified List, and Addition of Entity to the Military End-User List, 86 Fed. Reg. 36496 (July 12, 2021); Addition of Certain Entities to the Entity List, 86 Fed. Reg. 33119 (June 24, 2021); Addition of Certain Entities to the Entity List, Revision of Existing Entries on the Entity List, 85 Fed. Reg. 44159 (July 22, 2020); Addition of Certain Entities to the Entity List; Revision of Existing Entries on the Entity List, 85 Fed. Reg. 34503 (June 5, 2020); Addition of Certain Entities to the Entity List, 84 Fed. Reg. 54002 (Oct. 9, 2019).

<sup>6</sup> Addition of Entity to the Entity List, and Addition of Entity to the Military End-User List and Removals from the MEU List, 86 Fed. Reg. 4862 (Jan. 15, 2021), *revised*, 87 Fed. Reg. 38920 (June 30, 2022); Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities from the Entity List, 85 Fed. Reg. 83416 (Dec. 22, 2020); Addition of Entities to the Entity List, and Revision of Entries on the Entity List, 85 Fed. Reg. 52898 (Aug. 27, 2020).

<sup>7</sup> Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities from the Entity List, 85 Fed. Reg. 83416 (Dec. 22, 2020).

<sup>8</sup> Additions and Revisions of Entities to the Entity List, 88 Fed. Reg. 13673, 13674 (Mar. 6, 2023). The parent entity, BGI and another subsidiary, Beijing Liuhe BGI, were previously added to the Entity List in 2020 for "conducting genetic analyses used to further the repression of Muslim minority groups in the XUAR." Addition of Certain Entities to the Entity List; Revision of Existing Entries on the Entity List, 85 Fed. Reg. 44159, 44159-60 (July 22, 2020).

Where BIS cannot verify a company's bona fides, they may be added to the Unverified List (UVL).<sup>9</sup> Once on the UVL, a party is not able to use license exceptions, such as obtaining replacement parts for a previously exported item. Last fall, BIS added a rule that will put parties on the Entity List where there is sustained non-cooperation from the parties' host government on end-use checks.<sup>10</sup> The recent rule change properly and more aggressively targets these companies and foreign governments inhibiting end-use checks, giving the U.S. government another tool.

Begun in 1997, the Entity List then largely listed front companies for diversion and certain actors involved in proliferation-related activities. We have since moved to designating large companies and national champions in critical industries. Today there are 631 China-based parties on the Entity List.<sup>11</sup> BIS's continued use of the Entity List is a welcome development in aid of ensuring our technologies are not used for malign purposes, including against Americans.

The Entity List does have its shortcomings, however. By relying on a system targeting end-users, malign actors can play corporate shell games to circumvent the purpose of the listing. And although the regulations have a forward-looking element to permit listings where a party "poses a significant risk of being or becoming involved" in activities contravening the national security and foreign policy interests of the United States,<sup>12</sup> in my experience the listings are almost always for conduct that has already occurred.

Another shortcoming is that BIS lists out each subsidiary of a listed party, as well as the party's address. It certainly is not difficult to change a corporate name or address to evade the listing, something that is reportedly happening with one of the newest listed parties, Inspur.<sup>13</sup> As discussed below, it is worth exploring whether changes should be made to this process to ensure a more complete capture of related parties.

The U.S. government also should work to integrate the lists where possible, recognizing that each has different authorities. For example, the CMIC List administered by the Treasury Department targets companies supporting the military-industrial complex of the PRC.<sup>14</sup> It would seem that any company on that list, and therefore prohibited from listing on U.S. securities

---

<sup>9</sup> 15 C.F.R. part 744, Supp. 6.

<sup>10</sup> Revisions to the Unverified List; Clarifications to Activities and Criteria That May Lead to Additions to the Entity List, 87 Fed. Reg. 61971, 61972 (Oct. 13, 2022).

<sup>11</sup> Emily Kilcrease & Michael Frazer, Sanctions by the Numbers: SDN, CMIC, and Entity List Designations on China, CENTER FOR A NEW AMERICAN SECURITY (Mar. 2, 2023) (there are now "603 Chinese persons are included on the Entity List"); Additions and Revisions of Entities to the Entity List, 88 Fed. Reg. 13673 (Mar. 6, 2023) (adding an additional 28 Chinese parties to the Entity List).

<sup>12</sup> 15 C.F.R. § 744.11(b).

<sup>13</sup> Ian Talley, Asa Fitch & Clarence Leong, Loophole Allows U.S. Tech Exports to Banned Chinese Firm, WALL ST. J., Mar. 24, 2023, <https://on.wsj.com/3zw7nGD>.

<sup>14</sup> 31 C.F.R. part 586.

exchanges, would be acting contrary to the national security and foreign policy interests of the United States<sup>15</sup> and should therefore also be prohibited from receiving U.S.-origin technology.

The breadth and volume of additions to the list are an important tool in our national security toolkit. The U.S. government should take care to ensure that it is being sufficiently proactive and adding parties to the Entity List in a timely manner.

### **Foreign-produced Direct Product Rules**

The increased use of the Entity List has forced the U.S. government to likewise enhance some of the preexisting mechanisms of how to enforce it. One such example is the expansion of the Foreign-produced Direct Product Rule (FDPR).

Shortly after Huawei was added the Entity List, it became apparent that the U.S. government needed a better plan to inhibit circumvention of the prohibitions. The global nature of the semiconductor supply chain provided ample opportunity for Huawei and those interested in continuing to supply it to render the Entity List restrictions less potent. Under the initial listing, companies could simply move production offshore, effectively getting around the prohibition.

To counter that concern, the U.S. government determined that more action was needed and issued a new set of restrictions. What resulted was a set of two rules that, in short, limited Huawei's ability to source chips that were made with U.S.-origin design software or semiconductor manufacturing equipment, no matter where the chips were made.<sup>16</sup>

The use of the rule against Huawei paid almost immediate dividends. The United Kingdom reversed its earlier decision to permit Huawei into its telecommunications system, pointing to the FDPR as a reason for changing course.<sup>17</sup>

The FDPR has been applied several times since. Following Russia's invasion of Ukraine, the U.S. government used the FDPR across Russia and Belarus.<sup>18</sup> More recent actions also invoke the FDPR, including restrictions on advanced computing and supercomputers,<sup>19</sup> elements of the

---

<sup>15</sup> 15 C.F.R. § 744.11(b).

<sup>16</sup> Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule), 85 Fed. Reg. 51596 (Aug. 20, 2020); Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List, 85 Fed. Reg. 29849 (May 19, 2020).

<sup>17</sup> Press Release, United Kingdom, Department for Digital, Culture, Media & Sport, et al., "Huawei to be removed from UK 5G networks by 2027," July 14, 2020, <https://bit.ly/40RDQTB>.

<sup>18</sup> Expansion of Sanctions Against Russia and Belarus Under the Export Administration Regulations (EAR), 87 Fed. Reg. 22130 (Apr. 14, 2022); Implementation of Sanctions Against Russia Under the Export Administration Regulations (EAR), 87 Fed. Reg. 12226 (Mar. 3, 2022).

<sup>19</sup> Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification, 87 Fed. Reg. 62186, 62189 (Oct. 13, 2022).

supply chain of Iranian unmanned aerial vehicles sent to Russia,<sup>20</sup> and Chinese computing companies aiding in China's military modernization efforts.<sup>21</sup>

The FDPR was a sea change in how the U.S. government regulates the use of U.S.-origin technology. Although no system is perfect, the FDPR has made it more difficult for our adversaries to obtain our technology.

### **Military-Civil Fusion**

The CCP aims to develop the People's Liberation Army into a world-class military by 2049. As a result, it has embarked on a whole-of-government and whole-of-private sector effort to do so. That effort is personally overseen by CCP General Secretary Xi Jinping.<sup>22</sup> Given the rise of China's – and other foreign adversaries', for that matter – practice of MCF, the U.S. government recognized it needed to adapt export controls to meet the challenge.

As an export control problem set, MCF is among the most difficult. Particularly in a place like China, MCF challenges export-control licensing and enforcement, given the often unclear distinctions between civilian and military entities. In addition, the CCP is adept at transferring to its military technology developed and intended for use in the civilian arena.

In April 2020, BIS issued a rule to tighten controls on military end use and end users (MEU), applying a presumption of denial of licenses to such users.<sup>23</sup> Building upon a 2007 rule that imposed a license requirement on items intended for military end-use in China, the 2020 MEU rule expanded the license requirements to military end-users there and broadened the range of items subject to a license. It also warned exporters to China that the rule “will require increased diligence with respect to the evaluation of end users in China, particularly in view of China's widespread civil-military integration.”<sup>24</sup> The 2020 MEU Rule applied the controls to Russia and the Maduro Regime in Venezuela, in addition to China.

Following the 2020 MEU rule, BIS created a Military End User List (MEU List).<sup>25</sup> The MEU List aimed to help exporters know who the U.S. government viewed as MEUs and for whom a license would be required to export items. Importantly, it did not relieve exporters of the

---

<sup>20</sup> Export Control Measures Under the Export Administration Regulations (EAR) To Address Iranian Unmanned Aerial Vehicles (UAVs) and Their Use by the Russian Federation Against Ukraine, 88 Fed. Reg. 12150 (Feb. 27, 2023).

<sup>21</sup> Additions and Revisions of Entities to the Entity List, 88 Fed. Reg. 13673, 13674 (Mar. 6, 2023).

<sup>22</sup> U.S. Dep't of State, The Chinese Communist Party's Military-Civil Fusion Policy, undated, <https://bit.ly/3TpZMTb> (last visited Apr. 4, 2023).

<sup>23</sup> Expansion of Export, Reexport, and Transfer (in-Country) Controls for Military End Use or Military End Users in the People's Republic of China, Russia, or Venezuela, 85 Fed. Reg. 23459 (Apr. 28, 2020).

<sup>24</sup> *Id.* at 23460.

<sup>25</sup> Addition of “Military End User” (MEU) List to the Export Administration Regulations and Addition of Entities to the MEU List, 85 Fed. Reg. 83793 (Dec. 23, 2020) (adding 102 MEUs to the newly created list, including 57 from China).

obligation to conduct their own due diligence to ensure their items were not aiding these adversaries' militaries.<sup>26</sup>

A sampling of Chinese entities on the MEU list includes Aviation Industry Corporation of China, a state-owned military and civilian aerospace company, as well as a subsidiary of China State Shipbuilding Corporation, a company that builds ships for the People's Liberation Army Navy.<sup>27</sup>

The U.S. government's efforts to isolate known MEUs and provide guidance to the business community is a welcome development. But we must remain vigilant and modify the list as necessary. The government must also hold exporters to their obligations to conduct diligence on their shipments, particularly to China, but also to destinations that present a high risk of diversion.<sup>28</sup>

The U.S. efforts to impose a due diligence requirement on putative exporters to destinations with significant MCF is all the more important given the PRC's recent raid on a U.S. due diligence investigations firm.<sup>29</sup> If the CCP is going to inhibit on-the-ground diligence within the PRC, the U.S. government should require a greater showing to permit the shipment of sensitive items to the PRC.

### **Controls on indigenous Chinese semiconductor companies**

In October 2022, the U.S. government imposed perhaps the most impactful controls on the PRC's indigenous semiconductor industry.<sup>30</sup> Focusing on high-end AI chips and semiconductor manufacturing equipment, the rule aimed to implement National Security Advisor Sullivan's pronouncement that relative advantages are no longer sufficient.<sup>31</sup>

The rule imposed controls on items helpful to the PRC's advanced computing capabilities, which "are being used by the PRC for its military modernization efforts."<sup>32</sup> The efforts include the military's "autonomous military systems, such as those used for cognitive electronic warfare,

---

<sup>26</sup> Addition of "Military End User" (MEU) List to the Export Administration Regulations and Addition of Entities to the MEU List, 85 Fed. Reg. 83793, 83794 (Dec. 23, 2020) (noting the MEU List "is not exhaustive" and exporters "must still conduct due diligence for parties not on the list").

<sup>27</sup> 15 C.F.R. part 744, Supp. 7 (MEU List).

<sup>28</sup> 15 C.F.R. § 772.1 (defining "knowledge" under the EAR as not only "positive knowledge," but "also an awareness of a high probability of its existence or future occurrence," and prohibiting conscious disregard or willful avoidance of facts).

<sup>29</sup> Michael Martina & Yew Lun Tian, China detains staff, raids office of US due diligence firm Mintz Group, REUTERS, Mar. 24, 2023, <https://reut.rs/40o5uaX>.

<sup>30</sup> Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification, 87 Fed. Reg. 62186 (Oct. 13, 2022).

<sup>31</sup> Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit, THE WHITE HOUSE, Sept. 16, 2022, <https://bit.ly/3LXznuk>.

<sup>32</sup> Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification, 87 Fed. Reg. 62186, 62187 (Oct. 13, 2022).

radar, signals intelligence, and jamming” and designing and testing weapons of mass destruction, “hypersonics and other advanced missile systems.”<sup>33</sup> The rule imposed a foreign direct product control on several entities related to the PRC’s supercomputing capabilities.

The rule also imposed controls on certain semiconductor manufacturing equipment. Concerned about the military-modernization efforts relevant to the supercomputers controls in the preceding paragraph, the equipment-based control also flowed from concerns about the PRC’s nuclear expansion efforts.<sup>34</sup> The controls seek to limit indigenous Chinese semiconductor companies to two generations behind the current leading edge.

Similar to sanctions imposed by Treasury’s Office of Foreign Assets Control (OFAC), the rule also imposed a U.S.-person control.<sup>35</sup> The control was followed by an amendment to ECRA permitting control of U.S.-person activities to certain military, security, or intelligence services.<sup>36</sup> The October semiconductor control seeks to limit citizens, legal permanent residents, U.S. companies, and any person in the United States from assisting indigenous PRC semiconductors from working on leading-edge products.<sup>37</sup>

Following the unilateral imposition of these controls, the U.S. government worked to gain plurilateral acceptance with the Japanese and Dutch governments.<sup>38</sup> That reported success is important because those countries have companies that made some of the most competitive manufacturing equipment covered by the controls. Although the Dutch and Japanese controls are unlikely to match the full scope of the U.S. controls, it is likely that they will inhibit significant portions of the PRC’s indigenous semiconductor production. Had the U.S. government failed to secure agreement, the PRC would have been able to obtain the foreign items and evade the purpose of the controls.

The PRC is continuing to look for ways out from under the restrictions. Although comprehensive data are not available publicly, early indications are that the controls are working. There are reports that the PRC is responding to the controls on high-end chips by doubling down on making decade-old legacy chips to potentially flood world markets, an issue which presents its own set of problems.<sup>39</sup> These chips – defined at the 28 nanometer node or above – are embedded in a wide variety of automotive, weapons, and internet of things products. There are

---

<sup>33</sup> *Id.*

<sup>34</sup> *Id.*

<sup>35</sup> *Id.* at 62193.

<sup>36</sup> 50 U.S.C. § 4812(a)(2)(F), as amended by Pub. L. No. 117-263, § 5589(b) (2022).

<sup>37</sup> For the definition of “U.S. Person” under the EAR, see 15 C.F.R. part 772.

<sup>38</sup> Alexandra Alper & David Shepardson, U.S. official acknowledges Japan, Netherlands deal to curb chipmaking exports to China, REUTERS, Jan. 31, 2023, <https://reut.rs/40N79GD>; Tim Kelly & Miho Uranaka, Japan restricts chipmaking equipment exports as it aligns with US China curbs, REUTERS, Mar. 31, 2023, <https://reut.rs/3nMPpgi>.

<sup>39</sup> Jane Lee, et al., Analysis: China's massive older chip tech buildup raises U.S. concern, REUTERS, Dec. 13, 2022, <https://reut.rs/3GDcPz>; Sujai Shivakumar, The Strategic Importance of Legacy Chips, CENTER FOR STRATEGIC & INT’L STUDIES (Mar. 2023), <https://bit.ly/3KdcDns>.

also reports that the PRC has enlisted Alibaba and Tencent to assist in designing chips using open-source architecture to undermine the purpose of the controls.<sup>40</sup> The reports of state direction certainly give rise to the concern that any advancements could be used to further the PRC's military.

Time will tell on the ultimate effect of these controls. We must keep in mind that, like any export control, these controls will be time-limited and will need to be paired with efforts to run faster. The PRC is spending vast sums of money to try and build indigenously these machines and the products they make. The U.S. government and our partners, including the Dutch and Japanese, should continue to monitor the effectiveness of the controls.

### **Additional opportunities for success**

Although the U.S. government has made many significant and positive strides, there will always remain more work to be done. Simply put, China is a determined, persistent adversary unlike any the dual-use export control community has encountered before. Its practice of obtaining technology through IP theft, forced joint ventures, and non-traditional collectors around the world pose significant challenges.

Reports of U.S.-origin semiconductors being used to test Chinese hypersonic vehicles should concern us all.<sup>41</sup> A more recent example is reported links to a U.S. firm's subsidiary selling components that were found in the suspected Chinese spy balloon.<sup>42</sup> BIS did put several companies on the Entity List for supporting the Chinese balloon program, but the company mentioned in the news reporting was not one of them.<sup>43</sup> These two recent examples underscore the difficulty of a post-hoc enforcement after the items have been transferred; the technology is already in the hands of the adversary, and it has already been used against us. The government should rely more heavily on the "pose[s] a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States" portion of the Entity List rules.<sup>44</sup> The export-control interagency can then agree on a licensing policy consistent with the threat posed by the party.

I believe the October 2022 controls, particularly where supported plurilaterally by the Dutch and Japanese, will make it more difficult for the CCP to use our technology against us. The alignment and use of other U.S. government tools – like the Chinese Military Industrial

---

<sup>40</sup> Matthew Humphries, Following US Sanctions, China Decides Its Future Lies with RISC Chips, PC MAGAZINE, Dec. 2, 2022, <https://bit.ly/40VvE4E>; Anna Gross & Qianer Liu, China enlists Alibaba and Tencent in fight against US chip sanctions, FINANCIAL TIMES, Nov. 30, 2022, <https://on.ft.com/3U7SDam>.

<sup>41</sup> Ellen Nakashima & Gerry Shih, China builds advanced weapons systems using American chip technology, WASH. POST, Apr. 9, 2021, <https://wapo.st/3TJj3PP>; Cate Cadell & Ellen Nakashima, American technology boosts China's hypersonic missile program, WASH. POST, Oct. 17, 2022, <https://wapo.st/3TsBw2C>.

<sup>42</sup> Andrew W. Lehren, Dan De Luce and Yasmine Salam, U.S. firm's subsidiary sold electronics to Chinese defense firm linked to spy balloon program, NBC NEWS, Mar. 6, 2023, <https://nbcnews.to/3TBJMxt>.

<sup>43</sup> Additions to the Entity List, 88 Fed. Reg. 9389 (Feb. 14, 2023).

<sup>44</sup> 15 C.F.R. § 744.16.

Company List administered by the Treasury Department – is a force-multiplier to help stem the flow of items and funds from the United States destined for the Chinese military.

There are discussions about adding a fifth multilateral export-control regime related to the China challenge. Although I would welcome the opportunity for the United States to align with like-minded countries on the threat posed by the CCP, I remain unconvinced another regime-based-on-consensus system would be effective. Many of our allies in recent years have made great strides in recognizing the threats, but there is still too wide of a gulf to make a consensus-based regime workable.

Apart from the lack of consensus on what to do to meet the China challenge, some of our allies and partners lack the legal frameworks to impose controls similar to what we do in the United States. Although I am currently skeptical of a new regime, I strongly believe the U.S. government should work closely with our allies to help them align their legal authorities to use export controls to meet this new challenge. In doing so, we should offer drafting assistance, as well as share relevant intelligence to ensure our partners are armed with the information to make informed choices.

Where multilateralism may be insufficient, I am more optimistic that plurilateralism will work. My view is guided by the success of the FDPR and that of the October 2022 semiconductor controls. With respect to the former, the U.S. government assessed the market and determined that a unilateral semiconductor control as applied to Huawei would be workable. A second iteration of the FDPR saw more than 30 U.S. allies align, or agree to align, their controls to ensure their technologies would not feed the Russian war machine in Ukraine and potentially beyond. In addition, the reported plurilateral agreement between the United States, Netherlands, and Japan on the October 2022 controls shows promise. Although lacking in terms of speed and certainly not a panacea, plurilateral controls represent the new way forward.

### **Effectiveness in identifying and controlling technologies of concern**

The U.S. government works hard to identify and control technologies to destinations and entities of concern. It will surprise nobody, however, that the speed of technology moves far faster than the federal government. That challenge becomes even more acute when the government takes a technology to be controlled to one of the multilateral regimes, a process that can take several years.

Take for example the SMIC Entity Listing described above. That listing was designed to limit exports for items “uniquely required” to produce below 10 nanometers.<sup>45</sup> At the time, that was two generations behind the leading edge. But in the semiconductor industry, the speed of the technology moves quickly, and there is essentially a new technology node every two or so years.

The U.S. government generally does a good job identifying technologies of concern. The process relies heavily on the government research community, as well as the Department of Defense and the Intelligence Community. Two emerging technologies it struggles to identify and

---

<sup>45</sup> Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities from the Entity List, 85 Fed. Reg. 83416, 83417 (Dec. 22, 2020).

control are artificial intelligence (AI) and quantum computing. There are several reasons for this.

First, there is wide dispute of what is the state of the art and therefore worth controlling. In 2018, following the passage of ECRA, BIS issued an advanced notice of proposed rulemaking to learn more about certain emerging technologies; among them, AI and quantum computing.<sup>46</sup> Many of the comments BIS received disputed those were even emerging technologies.

A second problem is one of scoping. Few would likely argue that placing export controls on the voice assistant on one's phone is an effective use of BIS's and its partners' limited time. That calculation might change, however, if that same or similar technology would allow voice-command to launch munitions against troops on the battlefield.

Third, experts in these fields will often tell you there are many segments of each of these technologies where the United States is not in the lead and thus any export controls would be self-defeating. Although the United States leads in several quantum and AI-related technologies, we do not have a monopoly. Any controls must account for foreign availability or similar technologies, including from China.

Fourth and finally, the speed of the adoption of emerging technologies poses a challenge of identifying and controlling it at the right time. It is sometimes a difficult exercise to decipher the blurred lines between research and development of a technology and its adoption. It can also take time to determine whether that technology has military application. The government should take care not to inhibit research that allows us to run faster, but it should not be too hesitant to control where technologies would give our adversaries a military advantage detrimental to the United States or in furtherance of identified U.S. foreign policy.<sup>47</sup>

Unfortunately, I struggle to identify the appropriate scoping for AI and quantum computing. The easiest – though I am not sure the most effective – way to control it is through end-use and end-user controls, similar to the October 2022 semiconductor controls, and have a destination-based control at certain thresholds. It would be important to craft a licensing policy that accounts for foreign availability but ensures that we are imposing a license requirement on U.S.-origin items that may aid the PRC military and intelligence services.

### **Finding the right structure and process for dual-use export controls**

BIS and its interagency colleagues face a veritable deluge of licenses. In FY 2021, the most recent year for which data is publicly available, BIS processed 41,446 licenses.<sup>48</sup> Given the more aggressive use of the Entity List, the FDPR, Russia-related controls, and additional controls

---

<sup>46</sup> Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58201 (Nov. 19, 2018). Section 1758 of ECRA required the Secretary of Commerce to lead a “regular, ongoing interagency process to identify emerging and foundational technologies” essential to the national security of the United States. 50 U.S.C. § 4817(a).

<sup>47</sup> See, e.g., 50 U.S.C. § 4811(1).

<sup>48</sup> U.S. Dep't of Commerce, Bureau of Industry & Security, Annual Report to Congress Fiscal Year 2021, at 18 (BIS 2021 Annual Rep.), <https://bit.ly/3TyzNJe>.

on semiconductor and other computing-related items to China, the licensing trend has been upward. I expect that to continue.

The Commission should request a study of the utility of moving to a single licensing system. Given our adversaries' blending of civilian and military, we must ask ourselves whether the current export-control construct continues to make sense.

The current bifurcation also can yield uncertainty. For instance, in FY 2021, BIS worked with the State Department on 226 commodity jurisdiction requests.<sup>49</sup> These requests ask State and Commerce to determine whether a particular item is subject to State's rules relating to defense articles or services under the International Traffic in Arms Regulations or Commerce's EAR. They are complex undertakings and can be time-consuming, often taking several months.

Although I do not currently have a well-formed view of whether a single licensing system and/or agency makes sense, I do think it is worth study. I am mindful that Congress only five years ago passed ECRA on a bipartisan basis. That said, it has been a busy five years, as our adversaries have become increasingly aggressive. Being able to move at pace with the threats, while reducing uncertainty to the exporting community, should be the goal.

### **Enforcement is difficult but improving**

With the proliferation of rules, addition of parties to the Entity List, and expansion of the FDPR, BIS has its hands full with enforcement. To meet this challenge, BIS's enforcement has 30 domestic offices and soon to be 10 international offices at embassies and consulates, including in Beijing.<sup>50</sup> But only a fraction of licenses granted are subject to end-use checks. Of the 41,446 licenses granted in FY 2021, BIS completed 1030 end-use checks.<sup>51</sup>

As one can imagine, ensuring something as small as a semiconductor remains in the right hands is difficult. Indeed, in the wake of the October 2022 semiconductor controls, there are reports that Chinese AI companies on the Entity List are using intermediaries to rent or otherwise acquire chips that are export-controlled.<sup>52</sup> The task is made all the more difficult when one considers the steps BIS must take to conduct end-use checks in China, which include pre-approval from the PRC government, lengthy delays, and other bureaucratic obstacles. In some cases, the circumvention is state-backed, including reports that the October rules "prompted the proliferation of state-backed computer clusters, which stockpiled Nvidia chips and rented out access of the technology to blacklisted companies." It is difficult to imagine that the CCP would do so if not to assist its military, given its MCF policy.

---

<sup>49</sup> BIS 2021 Annual Rep. at 19.

<sup>50</sup> U.S. Dep't of Commerce, Bureau of Industry & Security, Organization, <https://bit.ly/3yZUhkN> (last visited Apr. 4, 2023); BIS 2021 Annual Rep. at 45-46.

<sup>51</sup> BIS 2021 Annual Rep. at 45.

<sup>52</sup> Eleanor Olcott, Qianer Liu & Demetri Sevastopulo, Chinese AI groups use cloud services to evade US chip export controls, FINANCIAL TIMES, Mar. 6, 2023, <https://on.ft.com/40dR4ts>.

Recent actions by BIS offer promise for tightened enforcement. In June 2022, BIS issued a memorandum pointing to increased use of “egregious” case designations, which can yield higher penalties; non-monetary settlements for less-significant cases, including required compliance program enhancements; elimination of no admit, no deny settlements; and publicly posting the charging letters.<sup>53</sup> The latter two, in particular, are welcome changes. Requiring violating parties to admit their wrongdoing and making their conduct public will serve an educational purpose and hopefully cause parties to reconsider before violating.

To meet the challenge of expanding controls, and the licenses they bring, BIS must be resourced adequately. In this stage of the great power competition era, BIS reminds me of Treasury’s Terrorism and Financial Intelligence (TFI) component in the wake of 9/11. We are aware of the problem, and hopefully like TFI, Congress will see fit to ensure BIS has the resources, both financial and interagency assistance, to meet the challenge. Significant investments in technology, particularly to harness the power of AI and big data analytics, are necessary.<sup>54</sup>

Congress should look at increasing the incentives for compliance. The current ceiling for a civil violation is \$300,000, adjusted for inflation, or twice the value of the transaction.<sup>55</sup> Parties who violate ECRA may also have their export privileges revoked.<sup>56</sup> Increasing the use of denial orders – which prohibit an offending party’s ability to export anything from the United States – would have a positive effect on incentivizing parties’ compliance with the rules.

Enforcement is and likely will always remain a challenge. The very nature of the items make diversion possible. Keeping penalties significant may further incentivize exporters to comply with the law.

### **Private-sector coordination is difficult to achieve, but a necessary part of the process**

The considerations in crafting and implementing national security rules, while simultaneously limiting collateral damage is perhaps the most difficult aspect of export-control regulation. The interaction between the government and the private sector is critical. Both sides have crucial expertise to help make policy: intelligence, geopolitical, and national security on the government side; and technological, market, and economic on the industry side. Each needs to be brought to bear to craft effective policy.

Unfortunately, the interaction between the government and the private sector is often less than ideal. It was the rare case that a company would come in and work to help shape potential controls on the front end. Industry is often reflexively and completely opposed to new controls.

---

<sup>53</sup> Mem. For All Export Enforcement Employees from Matthew S. Axelrod, Further Strengthening Our Administrative Enforcement Program, June 30, 2022, <https://bit.ly/3nbyrbm>.

<sup>54</sup> See, e.g., Gregory C. Allen, et al., Improved Export Controls Enforcement Technology Needed for U.S. National Security, CENTER FOR STRATEGIC & INT’L STUDIES (Dec. 2022), <https://bit.ly/3MiinPw> (recommending \$25 million annually for technology upgrades and staff increases, \$18.4 million and an additional 48 positions for enforcement).

<sup>55</sup> 50 U.S.C. § 4819(c).

<sup>56</sup> *Id.*

Instead, it was more often companies would come in after the release of a rule and offer helpful suggestions.

It is difficult to blame industry entirely. Because much of export control policy has inputs from intelligence and law enforcement sources, the conversations can often be one way. I was acutely aware of the disappointment during meetings when the government response was “we can’t tell you that” given the need to protect classified or other sensitive information.

Both during my time in government and now in the private sector, I have often thought about whether there is a better way for industry and the government to work together better. Often and quite understandably industry wants advance notice for planning purposes. It is difficult to do so, however. Providing advance notice would only exacerbate the stockpiling problem we have seen in some cases. For instance, it was widely reported that Huawei was stockpiling chips in advance of the FDPR.<sup>57</sup> It was only the end of 2022 – more than three and a half years after Huawei was added to the Entity List – that the company reportedly exhausted its stockpile.<sup>58</sup>

Regular engagement with industry is an important part of the process. The government should share information where it can, and I believe it does. Both sides must engage in good faith and with an understanding of the threats we face.

### **Recommendations for Congress**

As my testimony makes clear, there have been many recent successes in dual-use export control policy as it relates to China. But more can be done to ensure we retain the nimbleness to face a determined and persistent adversary.

#### **Study a single licensing system**

Although ECRA is less than five years old, Congress and/or the Commission would be wise to consider whether moving to a single export-licensing system makes sense. Particularly considering China’s and other adversaries’ MCF policies, having two different systems can yield consequential delays. These are delays we can ill afford when our adversaries are continuing to use any means to overtake us.

The Obama Administration launched a comprehensive export-control reform effort in 2009.<sup>59</sup> Notwithstanding the “byzantine amalgam of authorities, roles, and missions scattered around

---

<sup>57</sup> Lauly Li & Cheng Ting-Fang, Huawei builds up 2-year reserve of “most important” US chips, NIKKEI ASIA, May 28, 2020, <https://s.nikkei.com/40bOnZJ>.

<sup>58</sup> Iris Deng, Struggling Huawei runs out of advanced in-house-designed chips for smartphones amid US trade sanctions, Counterpoint report says, SOUTH CHINA MORNING POST, Dec. 21, 2022, <https://bit.ly/3n9PjPR>.

<sup>59</sup> For a good overview of the history of this effort, see generally The U.S. Export Control System and the Export Control Reform Initiative, CONG. RES. SERV., R41916, at 10-21 (2020), <https://bit.ly/3JWqJcZ>.

different parts of the federal government,”<sup>60</sup> the export-control reform effort did not make headway into implementing single-licensing system.

Any single licensing system should of course have all necessary intelligence inputs to ensure effectiveness. If it is determined that such a licensing system would be preferable, it is critical to ensure that the administering body be well-resourced and have all necessary authorities, as well as having the proper supporting analytic functions to bring together sufficient economic and technical data, intelligence collection, and open-source information.

### **Consider de-linking export controls from CFIUS**

As part of ECRA and FIRRMA, Congress decided to tie critical technologies and export controls to make certain CFIUS transactions mandatory. Although well-intentioned and done in lieu of adding an outbound investment review provision, the speed with which export controls and technology move is insufficient to meet the challenge.<sup>61</sup> The preference for multilateral controls slows the process of linking to CFIUS.

Rather, Congress should consider amending FIRRMA and putting sector-level review in place for certain sensitive technologies, no matter where the acquiring entity is based. It is tempting to create a foreign adversary list to tie to these sectors, but China’s increasing use of variable interest entities to shield the true nature of certain companies counsels in favor of sector-wide notification. The declaration process introduced in FIRRMA seems a good middle ground for notification, as opposed to a full notice. It would allow CFIUS to move quickly past filings that present little concern, while at the same time giving the government visibility into the transaction.

### **Consider a process that includes all of a party’s subsidiaries when being added to the Entity List**

The current process of adding parties to the Entity List is flawed in that BIS determines which of a party’s subsidiaries should be added to the list, as well as including the party’s address. That gets the burden backwards; if a party is on the Entity List, and an exporter seeks to send items to a “good” subsidiary, it should come to Commerce and make the case.

The OFAC 50 Percent Rule provides an instructive example. OFAC rules prohibit doing business with any affiliate of a blocked party where the blocked party owns 50 percent or more of the affiliate.<sup>62</sup> OFAC additionally advises U.S. persons “to act with caution” when dealing with a non-blocked entity where a blocked person is affiliated, even at less than 50 percent.

---

<sup>60</sup> *Id.* at 10 n.19 (quoting Secretary of Defense Robert M. Gates, speech before the Business Executives for National Security, April 20, 2010).

<sup>61</sup> The Commission has heard from other witnesses suggesting this proposal, including by one of my NSI colleagues. *See* Testimony of Giovanna Cinelli, Fellow, National Security Institute, George Mason University Antonin Scalia Law School, at 12 (Sept. 8, 2021), <https://bit.ly/40ptudw>.

<sup>62</sup> Dep’t of the Treasury, Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property are Blocked, Aug. 13, 2014, <https://bit.ly/3FIjGmV>.

BIS could adopt a similar posture of putting all subsidiaries of a party on the Entity List or the MEU List or doing so at some prescribed threshold. For administrative purposes, it would be preferable to put all subsidiaries on, regardless of ownership threshold. Putting the burden on the exporter seeking to do business with a listed party is a reasonable step.

Adding parties to the Entity List is a time- and manpower-intensive process, and one that should harness big data analytic capability. The process today is entirely too reliant on manual inputs. Although we want to ensure we are putting eyes on the most relevant information, much of it can be culled by analytic programs that exist elsewhere. In addition, given the shift in the kinds of companies being added, the litigation risk is much higher than before. It is even more important that the agencies involved have considered sufficient information and build the file to withstand a potential court challenge.

It is important to use all of those tools to ensure that parties added to the Entity List are done so in a way that captures the national security threat and does not permit shell games to avoid the effect of the listing.

\* \* \*

As discussed above, the export-control landscape with respect to the PRC has shifted markedly in recent years. Our government and industry have shifted, too, and they must continue to adapt to this new normal.

I often said when I was in government that I was privileged to work on an area with such bipartisan agreement. That will be important as we go forward and Congress and the executive branch continue to refine our export-control system to meet the challenges ahead.

I look forward to your questions.