May 11, 2023

Statement of Hon. Nazak Nikakhtar[1]

Partner, International Trade and National Security Practice Chair, Wiley Rein LLP
Former Assistant Secretary for Industry & Analysis, Under Secretary for Industry & Security*
U.S. Department of Commerce

**Testimony Before the House Foreign Affairs Committee,
Subcommittee on Oversight and Accountability**

Reviewing the Bureau of Industry and Security, Part I: U.S. Export Controls in an Era of Strategic Competition

Chairman Mast and Ranking Member Crow, Committee members, experts, policy advisors, and staff, thank you for the opportunity to speak about the growing challenges posed by the People's Republic of China ("PRC") and other countries of concern to U.S. and global national security and economic security interests, and the appropriate U.S. Government response through the export control policies.

My name is Nazak Nikakhtar, and it is an honor to appear before you today. I am an international trade attorney and Chair of the National Security practice at the Washington, DC, law firm of Wiley Rein LLP. I am also a trade and industry economist, a former Georgetown University adjunct law professor, and recently completed my second tour of duty in the U.S. Government. Twenty years ago, I began my career as an analyst at the Department of Commerce's Bureau of Industry and Security and subsequently at the International Trade Administration ("ITA"), where my colleagues and I witnessed from the frontlines the predatory economic tactics used by our adversaries to acquire our technologies and ultimately erode our

[1] *The views and opinions expressed in this testimony are mine only and do not represent the views of Wiley Rein LLP or any of the firm's clients.*

industries. In 2004, I helped establish and lead the Commerce Department's "China/Non-Market Economy Office" and, for several years thereafter, I audited numerous foreign companies and their affiliates for the Department. In 2018, I returned to the Commerce Department to serve as Assistant Secretary for ITA's Industry & Analysis, and in 2019, I simultaneously performed the non-exclusive functions and duties of the Under Secretary for the Bureau of Industry and Security ("BIS"). It is from all of these vantage points that I offer my testimony and observations today about the risks to U.S. national and economic security arising from gaps in U.S. export control laws that must be closed to better address these risks. There are many.

I. INTRODUCTION

The scope of this testimony is focused on the national security risks posed by entities located in and/or subject to the jurisdiction of the governments[2] of foreign countries of concern and the appropriate U.S. Government response through export control laws and regulations. While I advocate for greater technology integration and the promotion of interoperability with America's friends and allies, I have become increasingly concerned about our adversaries' ability to obtain U.S. technology for weaponization against the United States and our partners – both military and economic weaponization. This is why I am advocating today for stricter export controls on goods, software, and technology (collectively "items") to foreign countries of concern. I want to stress that my presentation is not about every nation but is limited to those that wish to harm the United States and our allies. In addition to the PRC, those nations include the Russian Federation, the Republic of Cuba, the Democratic People's Republic of Korea, and the Islamic Republic of Iran. Because most of these countries are subject to U.S. sanctions,

[2] Whether central, provincial, or local.

either comprehensive or substantial, U.S. transactions with these specific countries are small. Therefore, the focus of my testimony will be the PRC, the United States' third largest trading partner and the world's most significant technology transfer threat.

II. TECHNOLOGY COMPETITION AND NATIONAL SECURITY RISKS

Over the past two decades, technology transfers by America and its allies have helped accelerate adversary nations' technological and weapons capabilities. Examples include the PRC's dramatic leaps forward in semiconductor design and fabrication, battery energy storage and nuclear weapons capabilities, biotechnologies, artificial intelligence, space and aerospace engineering, and hypersonic weapons deployments. At the same time, the United States has systematically failed to protect its most critical assets. Rather than promulgate policies to better prevent technology transfer to adversary nations, the U.S. Government either ignored the problem or, worse, from approximately 2009 through 2016, instituted a government-wide "Export Control Reform" process that, in many instances, loosened the Export Administration Regulations ("EAR") governing exports of dual-use items to facilitate technology transfer to adversaries, either directly or indirectly through third-country transfers. Those reforms, still present in the U.S. Department of Commerce's EAR, need to be reversed.

Much of America's flawed thinking with respect to the export control process has been rooted in the notion that we need to transfer technology to foreign adversaries in exchange for cash, and that we would invest the cash to spur innovations at home that enable the U.S. to "run faster." But this approach has been failing for decades. The approach overlooks the PRC's massive industrial subsidies that far exceed any level of revenue that individual U.S. companies would ever be able to receive from exports to the PRC. The PRC has been running faster, benefitting from its massive workforce, technology misappropriation practices, and massive

subsidies, and now it is neck-in-neck with the United States. And in many instances, it has now leaped ahead, surpassing the United States and the rest of the world in 37 of the 44 key technologies that are likely to propel innovation, growth, and military power in the coming decades, including artificial intelligence, robotics, biotechnology, advanced manufacturing, and quantum technology.[3] And the PRC is leveraging its technological might and extensive control over the world's supply chains to threaten America and its allies both militarily and economically.

Surprisingly and very unfortunately, America has been unwilling to learn from its mistakes. The allure of short-term profits from abroad has been too great to compel industries and the U.S. Government to take action to protect the nation's medium- and long-term interests. Today, American corporations are continuing to eagerly transfer their innovations to the PRC in exchange for temporary access to the revenue stream available from PRC market. Further, and more profoundly, America's addiction to the PRC revenue stream has become so severe that much of America has forgotten what it was like to be truly independent of the PRC – a reality that had once underpinned American strength and prosperity 20 years ago, but shortly ended after the PRC's accession to the World Trade Organization ("WTO").

Without question, the appeal of transferring technology to the PRC for some small earnings has gripped our national identity so strongly that we have lost touch with the true notion of competition that once compelled America to innovate with the objective of building domestic capabilities in order to leverage global economic strength. Instead, we have been operating

---

[3] Dr Jamie Gaida et al., *ASPI's Critical Technology Tracker*, Australian Strategic Policy Institute (Mar. 02, 2023), https://www.aspi.org.au/report/critical-technology-tracker.

under the invisible and manipulative hand of the PRC's tech-for-cash scheme that has significantly weakened the U.S. industrial and innovative base.

Today, American corporations continue to organize and re-organize themselves for the primary purpose of trading with and transferring sensitive technology to the PRC. For these American corporations, the PRC began replacing American and other third-country markets as their primary sources of sales revenue in the early 2000s, and since then, America's export dependence on PRC revenue has only increased. This is precisely the reason why corporations lobby so aggressively for continued access to the PRC's markets.

In fact, lobbying efforts have succeeded so well that the U.S. Government has fallen into a pattern of ceding vital national security interests in exchange for the American industry's market access. Lobbying has also given rise to the concept of "nuanced" trade policies that aim to minimize regulations while maximizing business opportunities abroad. Again, these policies are "nuanced" by design, by thinly regulating trade (to create the appearance of protecting national security) while simultaneously creating carveouts for substantial business interests with the PRC for fear of backlash by industry and Wall Street if rules become too prohibitive.

Bizarrely, the U.S. Government remains committed to this policy approach even though history has repeatedly proven that the PRC manipulates legal "nuances" to its advantage and to America's detriment. Case in point: the PRC's violation of virtually every trade pact it has entered into to date, including its violation of bilateral and multilateral intellectual property ("IP") rights agreements, repeated circumvention of U.S. sanctions and export control laws, predatory economic practices that undermine fair trade agreements, and the deliberate influence and coercion over international standards organizations. Indeed, because the Chinese government and the Chinese Communist Party exercise extensive control over all PRC

businesses, they are able to direct corporate behavior in a coordinated manner that substantially undermines "nuanced" U.S. regulatory action.[4]

To be blunt, our export control system has failed to adequately curb the transfer of critical assets and technologies to foreign adversaries. In fact, the EAR is replete with gaps intended to permit an enormous range of transactions with the PRC and other foreign countries of concern while restricting exports in very limited, narrow, and isolated ways. The fact that approximately 0.4% of U.S. exports worldwide, and only 0.7% to the PRC, require an export license makes this point amply clear.[5]

To be sure, wherever there are gaps in our laws, PRC entities circumvent those gaps by acquiring prohibited goods, technologies, and software through in-country intermediaries that are exempt from the narrow scope of the rules. In many other instances, PRC entities outrightly violate the rules themselves. Enforcement is nearly impossible given the massive size and scale of industries and operations across the PRC, the PRC government's elaborate circumvention strategies, and transparency difficulties in dealing with the opaque PRC regulatory system.

Mounting evidence in the press now shows just how much sensitive technology the PRC has been acquiring despite the United States' export control system. In the critical semiconductor industry, it was reported last year that the PRC's acquisition of sensitive U.S. integrated circuit ("IC") design and technology enabled it to race ahead of the United States in

---

[4] Specific, additional examples include the undermining of the Huawei Technologies Co., Ltd. Entity Listing through affiliate Honor and the circumvention of U.S. export control laws to supply technology to the Russian Federations to support its sustained war against Ukraine and technology to the Islamic Republic of Iran to continue the oppression of its population.

[5] *BIS U.S. Trade With China 2022 Report,* available at https://www.bis.doc.gov/index.php/country-papers/3268-2022-statistical-analysis-of-u-s-trade-with-china/file#:~:text=In%202022%2C%20for%20tangible%20items,totaled%20980%20for%20%2425.4%20billion..

hypersonic flights and weapon systems development. Further, it is also well-documented that the PRC has rapidly advanced its semiconductor capabilities through technology transfer such that it is now ahead of the United States both in IC manufacturing capacity and capabilities at the leading-edge nodes of 10 nm and below. These ICs enable dangerous supercomputing capabilities, advance the development of weapons of mass destruction, and enhanced the PRC government's surveillance capabilities both within China and abroad. Equally problematic is the fact that the PRC also diverts U.S. exports of ICs and other technology to assist foreign adversaries, including sanctioned Russian and Iranian entities, to produce highly advanced weapons and aircraft. In this way, the PRC's technology acquisition indirectly contributes to the death of hundreds of thousands of innocent people. The U.S. system of enabling the PRC and other adversaries needs to change.

It is time to rethink our strategy of exporting technology to the PRC in exchange for revenue. In 2018, the Export Control Reform Act of 2018 ("ECRA") gave the Commerce Department's BIS permanent statutory authority to regulate exports of dual-use items, specifically goods, software, and technology.[6] ECRA also mandated that BIS improve its controls over exports of emerging and foundational technologies, recognizing that technology flows to the PRC and other malign actors needed to be reined in.

ECRA provides the foundation for BIS's ongoing work, but I also have been quite candid in asserting that the U.S. export control system for dual-use items needs an overhaul to more proactively address the risks posed by the PRC and other foreign countries of concern. What we have done to date is inadequate, as evidenced by the PRCs continued technological rise and

---

[6] Export Control Reform Act of 2018, H.R. 5040, 115th Cong.

Russia's and Iran's acquisition of U.S.-origin technology through the PRC. The United States needs stronger rules to protect technology transfer to adversaries and, simultaneously, to promote technology integration and interoperability with allies. It is why I appreciate the Committee's time to have this important hearing today, and I hope that the Committee finds these recommendations helpful.

III. SPECIFIC RECOMMENDATIONS

A. Transparency With Respect to Commerce's General Licensing Policy

The Department of Commerce, specifically through BIS, regulates exports of items – specifically goods, software, and technology – through export control licenses under the EAR. Items that BIS deems to be most sensitive are identified on a positive control list – the "Commerce Control List" ("CCL"), which describes through technical specifications particular items that are subject to licensing requirements for exports, unless an exception applies. Each item is identified by a specific Export Control Classification Number ("ECCN") and accompanying licensing policy. BIS also regulates exports to prohibited end uses (e.g., weapons of mass destruction, nuclear capabilities, and chemical and biological weapons) as well as to restricted end users (e.g., Entity List and military end users). Exports are either (1) subject to a license, (2) qualify for a license exception, or (3) do not require a license at all.

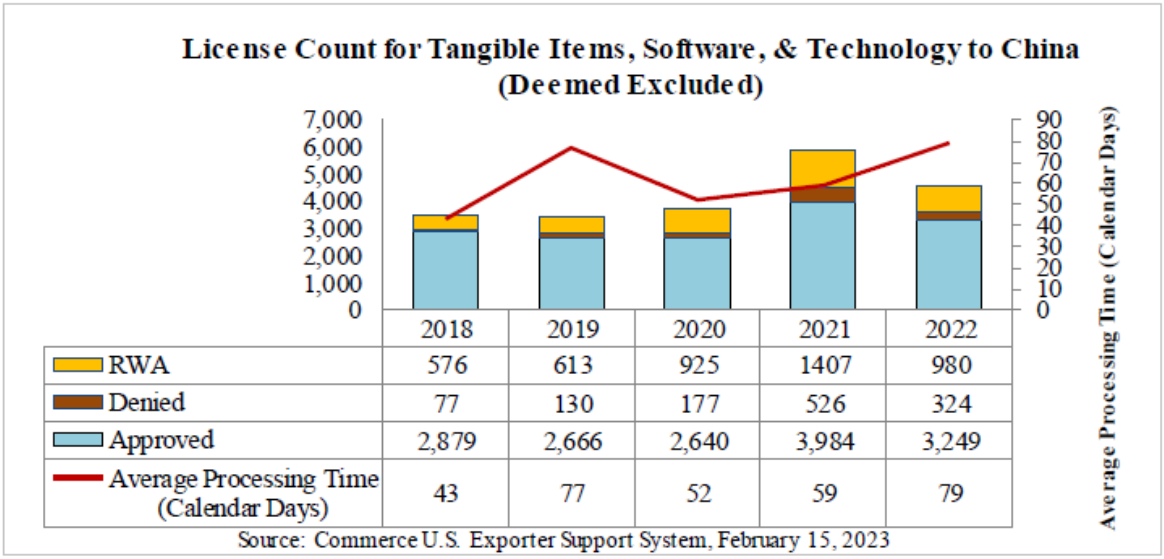
The Commerce Department issues reports to Congress each year outlining its licensing statistics and trends. These reports would be extremely useful for Congressional oversight and general public awareness if they were less opaque. Each year, BIS's annual reports obscure licensing trends by providing data at too high of an aggregated level to be useful in measuring the effectiveness of BIS's export control license policies. For instance, the reports produce the general statistics shown in the table below but do not specify exports by identifying how many

entities in foreign countries of concern received licensed items, the nature of those entities (for example, state-owned enterprises, military affiliates, or Entity Listed companies), the specific types of items that were exported (comprehensively, by full ECCNs), or the types of exported items that fell outside licensing requirements.

The tables below depict the aggregated data that BIS reports to Congress each year.[7]

Year	Total Licenses	Change from Prior Year	Approvals	Returned Without Action (RWA)	Denials	ECCN with Most Highest Approval
2017	34,142	+1.6%	28,891 (84.6%)	4,949 (14.5%)	302 (0.9%)	ECCN 9A610 (Military aircraft and related items), $10.1 Billion, 5,631 licenses
2018	35,346	+3.5%	30,379 (85.9%)	4,686 (13.3%)	281 (0.8%)	ECCN 9A610 (Military aircraft and related items), $12.6 Billion, 5,288 licenses
2019	34,207 $486.8 B	-3.1%	29,327 (85.7%)	4,561 (13.3%)	319 (0.9%)	ECCN 9A610 (Military aircraft and related items), $9.4 Billion, 5,075 licenses
2020	37,895 $173.7 B	+10.8%	32,687 (86.3%)	4,754 (12.5%)	454 (1.2%)	ECCN 9A610 (Military aircraft and related items), $14.7 Billion, 4,994 licenses
2021	41,446 $1.3 T	+8.6%	35,630 (86.0%)	5,109 (12.3%)	707 (1.7%)	ECCN 9A610 (Military aircraft and related items), 5,265 licenses

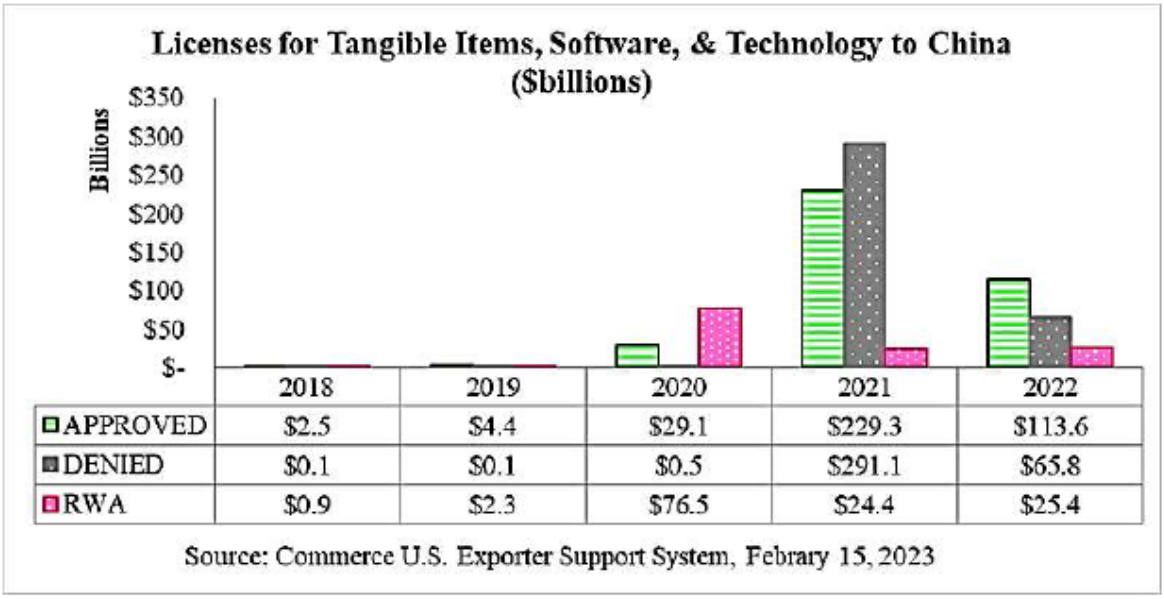
[7] Bureau of Industrial Security, *Publications*, https://www.bis.doc.gov/index.php/about-bis/newsroom/publications (last visited on May 9, 2023).



	2018	2019	2020	2021	2022
RWA	576	613	925	1407	980
Denied	77	130	177	526	324
Approved	2,879	2,666	2,640	3,984	3,249
Average Processing Time (Calendar Days)	43	77	52	59	79

Source: Commerce U.S. Exporter Support System, February 15, 2023

Deemed Export Licenses for Nationals of China						
2018-2022						
Year	Approved	RWA	Denied	China Total	World Total	China Total/ World Total
2018	306	59	0	365	967	37.7%
2019	541	72	0	613	1,302	47.1%
2020	400	49	3	452	1,212	37.3%
2021	254	20	0	274	928	29.5%
2022	479	32	0	511	1,462	35.0%



	2018	2019	2020	2021	2022
APPROVED	$2.5	$4.4	$29.1	$229.3	$113.6
DENIED	$0.1	$0.1	$0.5	$291.1	$65.8
RWA	$0.9	$2.3	$76.5	$24.4	$25.4

Source: Commerce U.S. Exporter Support System, Febrary 15, 2023

Again, as these statistics provide no visibility into the specific types of items that have been exported to foreign countries of concern, they need to be disaggregated in prior and future reports. BIS needs to disaggregate the data in ways that would allow Congress and the public to have a better sense of the specific goods, software, and technologies that are being licensed to foreign countries of concern, as well as general, non-proprietary information about those foreign end user recipients. This level of visibility is reasonable and is essential to evaluating U.S. national security risks and the effectiveness of U.S. export control policies. Indeed, if certain exports are important enough to be subject to licensing requirements, then Congress and the public need better information as to where they are going and to whom.

It should also be emphasized that the licensing statistics presented above are, on their face, extremely problematic. Since many exports to U.S. allies fall under the EAR's license exceptions, only the most sensitive exports to the most sensitive end-users or destination countries are subject to the EAR's licensing requirements. In light of this fact, it appears extremely problematic that BIS denies licenses for only 0.8% to 1.7% of license applicants overall, and approves well over 90% of export licenses to the PRC. These figures exclude instances where licenses are not required or license exceptions apply, making the approval rate substantially higher. Statistics this low warrant further investigation into the risks posed by BIS's licensed technology transfers to foreign countries of concern through license approvals, exemptions, and instances where lo licenses are required.

BIS's Return Without Action ("RWA") statistics should be better probed as well. RWAs may occur when license applications contain a mistake or when license applications are not required under the EAR. But the RWA system is also subject to abuse. It has been the case that, in order to avoid disputes among federal government officials about the adjudication of a specific

license, the license would be returned by an export licensing officer to the applicant through an RWA designation. Subsequently, upon receipt of the RWA, the applicant may either elect to refrain from exporting the item (given that it has not received explicit authorization by BIS), or it may proceed with the export (given that the RWA is not an express license denial). Both situations occur. Congress should better understand the basis for RWAs by ensuring that BIS's annual reports explain the reasons for RWAs each year.

It is also worth noting the values of U.S. exports as listed in BIS's annual reports may be unreliable because they are prone to understatement. License applicants may report understated values for controlled items for a variety of reasons, including when they are bundled with other items that are exempt from license requirements. For example, an applicant may report that the value of controlled software is $1 when the export value of the underlying product (e.g., a gaming computer not controlled under the EAR) incorporates the full value of the software as a bundle with the computer. Because Congress obviously needs to have a better understanding of the values associated with U.S. exports, the licensing process needs to be improved by BIS. BIS officials must work with license applicants to better ascertain the values of the proposed exports and capture improved value data in its internal records and annual reports to Congress.

Beyond annual reports, which are made public, the Commerce Department should also provide additional, confidential licensing statistics to the appropriate oversight committees in Congress. Licensing data are currently housed in the U.S. Government's Automated Export System ("AES").[8] This is a nationwide electronic system that must be completed by every U.S. exporter. The system requires specific information about the exporter, the destination country,

[8] U.S. Customs and Border Protection, *AES: An Introduction*, (May 24, 2022), https://www.cbp.gov/trade/aes/introduction.

the recipient, the consignee, the shipper, a description of the export, the relevant Harmonized Tariff System code, the ECCN, the volume and value of export, whether or not the export is subject to licensing requirements, and whether an export license was granted by the U.S. Government (by listing the license number).

The fact that this system is electronic makes the accumulation and sharing of information with Congress simple and expeditious.[9] Congress could request this data for exports of sensitive technologies to countries of concern on a regular basis as part of its oversight process. Data on exports that are exempt from licensing requirements and those that do not require licenses would also be instructive and relevant to Congress's oversight duties. Congress should again be mindful of the fact that values may be understated significantly and rely on other metrics (such as the number of licenses and the criticality of the exported technology) to evaluate the effectiveness of BIS's export control process.

B. Greater Transparency for Items Subject to Controls and Those Exempt

As noted, one of the Commerce Department's most important roles in the protection of national security is BIS's identification of emerging and foundational technologies for export control. When Congress passed ECRA, it understood that BIS needed to make better and more rapid progress in the identification of such technologies and so made this requirement explicit. To date, however, BIS has only identified just a few (roughly 50 or so) technologies for control. Juxtaposed against the vast number of technologies that are still not controlled, this is not a significant number. In the Appendix provided hereto, my testimony last year to the Senate

[9] AES is the dataset that is generated to produce the publicly-available annual reports to Congress, and when country-specific data are produced according to ECCN as explained above, confidential business information regarding the identities of the exporter and recipient could be kept confidential.

Select Committee on Intelligence, I provided recommendations on how BIS may improve the process of identifying emerging and foundational technologies for control. I incorporate those recommendations here by reference.

1. Understanding the Scope of Controls

While much work remains on BIS's identification of emerging and foundational technologies for control, the issue I want to focus on today is oversight. The fact that it is currently impossible for any person who is not also an engineer to determine, with any degree of reliability or certainty, the scope, coverage, and commercial significance of EAR controls is enormously troubling. The highly technical descriptions associated with each ECCN impede any meaningful oversight by Congress or the public at large. This needs to change.

A better way to provide transparency is for BIS to supplement ECCN descriptions with simpler descriptions. By analogy, the Commerce Department's ITA – BIS's sister bureau – issues very clear *product scope* language for its trade remedy cases that are straightforward, easy to understand, and clearly delineate the extent to which specific imports are subject to trade tariffs and those that are not. The State Department's U.S. Munitions List ("USML") under International Traffic in Arms Regulations ("ITAR") is fairly straightforward to understand as well. The same approach can and should be adopted for the ECCNs in the CCL.

Going forward, the BIS should produce, simultaneously with each new ECCN entry, a scope description that is drafted in such a way that allows policymakers to demarcate the types of goods, software, and technology that are subject to controls and those that are not. Such a common-sense approach would allow Congress, other federal government officials, and the public to have better visibility into how the Commerce Department is protecting national security interests.

For the ECCNs that already exist on the CCL, moreover, BIS should produce such scope descriptions as well. Given the current number of ECCNs, the agency could produce and publish scope descriptions over the course of a year. This level of effort is justified, given the transparency it would provide to policymakers and the public at large.

2. Enabling Broader Input for Controlling Emerging/Foundational Technologies

Currently, BIS identifies technologies that merit control under the EAR with some input from the federal agencies involved in the export control licensing process, including the U.S. Departments of State, Energy, and Defense, and sometimes the White House's National Security Council. However, there are additional stakeholders beyond this narrow group of federal agencies that should have the opportunity to inform the list of items subject to the EAR's export controls as well.

One option is for BIS to launch an open, transparent process by which industry participants, private entities, universities, and branches of the Government may submit nominations for emerging/foundational technologies for control. There are enough stakeholders with interest in protecting U.S. national security within these groups that would give rise to solid recommendations. I interacted with many of these entities during by time at BIS and ITA, and currently do so in private practice.

After a reasonable adjudication period, BIS should then be required to release public summaries of the items nominated for control (while maintaining the confidentiality of the submitters' identities) with an explanation of its ultimate decision to impose/not impose controls and its reasons. Additionally, an interagency committee should institute a mechanism whereby BIS's decisions may be challenged by any submitter on a confidential basis, and the committee

would serve as the neutral arbiter. Again, transparency of this kind is necessary for matters that involve important national security interests.

C. Emerging and Foundational Technologies Not Yet Controlled are EAR99

Under the EAR, items that are not identified for controls through ECCN designations under the CCL are classified as "EAR99." For EAR99 items, generally, a license is not required to export and re-export/transfer the products worldwide. According to BIS, EAR99 is typically comprised of low-technology consumer products and services:

- Most of the products, services, and technologies that fall within the scope of the EAR are not specifically controlled for export, and are given the classification of EAR99. They fall under U.S. Department of Commerce jurisdiction and are not listed on the CCL. EAR99 items generally consist of low-technology consumer goods and do not require a license in most situations.
- EAR99 items can generally be exported without a license but exporters of EAR99 items still need to perform careful due diligence to ensure that the item is not going to an embargoed or sanctioned country, a prohibited end-user, or used in a prohibited end-use.[10]

In short, the EAR99 category represents the lowest level of control.

The key point to emphasize here is that EAR99 items do not require licenses for export to most entities located in foreign countries of concern, including the PRC and other countries that routinely serve as points of diversion to Russia, Iran, North Korea, and Cuba. This is enormously problematic because all emerging and foundational technologies – including emerging and foundational technologies that have still not made their way to the CCL – are designated as EAR99 by BIS. This means that they are freely exported with the lowest licensing requirements. The fact that licensing requirements for the nation's most sensitive and dangerous

[10] International Trade Administration, *Export Control Classification # (ECCN) and (EAR99)*, https://www.trade.gov/eccn-and-export-administration-regulation-ear99 (last visited May 9, 2023).

technologies are no different than current license requirements for innocuous items such as tables and chairs is absurd. This needs to change.

D. Improvements to the Entity List System

BIS publishes the names of certain foreign entities that have likely been engaged in activities that could undermine or threaten U.S. national security or foreign policy interests on the EAR's Entity List. When designated to this List, both exports of sensitive technologies and yet-to-be-controlled emerging and foundational technologies (i.e., EAR99 items) to these entities are subject to BIS's license review process. The impact of designation on the Entity List can be enormous, as businesses may lose customers, revenue, and market share as a result of the U.S. Government's determination that the businesses are untrustworthy actors.

Moreover, the regulations governing the Entity List stipulate a very low legal threshold for designation and the process for designation is straightforward. According to BIS:

> The Entity List (supplement no. 4 to part 744 of the EAR) identifies entities for which there is reasonable cause to believe, based on specific and articulable facts, that the entities—including businesses, research institutions, government and private organizations, individuals, and other types of legal persons—that have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States. Parties on the Entity List are subject to individual licensing requirements and policies supplemental to those found elsewhere in the EAR.
>
> Entity List additions are determined by the interagency End-User Review Committee (ERC), comprised of the Departments of Commerce (Chair), Defense, State, Energy, and where appropriate, the Treasury.
>
> The ERC makes decisions regarding additions to, removals from, or other modifications to the Entity List. The ERC makes all decisions to add an entity to the Entity List by majority vote and makes all decisions to remove or modify an entity by unanimous vote.[11]

---

[11] See, e.g., Bureau of Industry and Security, Office of Congressional and Public Affairs, *Commerce Adds Eleven to Entity List for Human Rights Abuses and Reaffirms Protection of Human Rights as Critical U.S. Foreign Policy Objective*, (Mar. 30, 2023),

Thus, the Entity List is a powerful tool. It should be used more aggressively to counter the national security threats posed by entities abroad. And it should also be improved to be more effective. Several points are thus in order.

1. Increase Entity List Designations

First, there are currently approximately 2,404 entities on the Entity List in total, including 586 PRC entities and 816 Russian entities (inclusive of affiliates). But in the context of all Russian and PRC businesses more broadly, there are substantially many more entities that "pose significant risks of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States." Those entities merit designation to the Entity List, as well as every entity in the PRC and Russia that supports the state's military apparatus, directly or indirectly.[12] In fact, there is no rational reason why exports of U.S.-origin goods, software, and technology should continue making their way to these entities at all. The Entity List designation should be used to restrict such U.S. exports.

As to concerns that entities may threaten to litigate their designation to the Entity List, this fear should not drive inaction. The U.S. Government's priority should be to protect national security interests and to simultaneously defend its actions whenever appropriate. Fear of

https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3256-2023-03-30-bis-press-release-human-rights-entity-list-additions/file.

[12] They should also be designated on the Department of Defense's Chinese Communist Military Company list pursuant to Section 1260H of the 2021 NDAA, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R. 5395, 116th Cong. § 1260H, and the Department of Treasury's Chinese Military-Industrial Complex list as well, Dep't of the Treasury, Office of Foreign Asset Control, *Non-SDN Chinese Military-Industrial Complex Companies List*, (Dec. 16, 2021), https://www.treasury.gov/ofac/downloads/ccmc/nscmiclist.pdf.

litigation cannot be part of the Government's decision-making, as that can be manipulated by adversaries.

As already noted, the legal threshold for designation to the Entity List is very low by design, making the List an effective tool in preventing foreign malign actors from receiving critical U.S. technology. Accordingly, the list should be used aggressively and not sparingly. There can be no compromise when national security interests are at stake.

2. More Robust Designation of Subsidiaries and Affiliates

Next, the U.S. Government needs to more robustly designate affiliates of Entity Listed companies to the Entity List. Obviously, it would make little sense to designate a parent company yet exclude the subsidiaries and affiliates that are subject to the parent's direction and control. To illustrate this point using Huawei Technologies Co., Ltd., it defies logic that the U.S. Government continues to exclude Huawei's affiliate Honor from the Entity List, given substantial information about Honor's activities in aiding Huawei's acquisition of U.S. exports in circumvention of the Entity List prohibitions.[13]

Furthermore, in light of the fact that, in the PRC as well as Russia, the central government has absolute control over all political and economic activities and routinely compels companies to circumvent foreign laws to support the state's malign objectives, the U.S. Government must take seriously the fact that circumvention of the Entity List is commonplace – and even more so compulsory. More robust designations of subsidiaries and affiliates to the Entity List merit consideration.

---

[13] Basil Kronfli, *Honor May Not Be as Free From Huawei as it Claims*, Wired (Nov. 7, 2021), https://www.wired.com/story/honor-huawei-smartphones-separation/.

But practically, how can this be achieved? The answer is simple and has substantial precedent in law. Again, looking to trade as an analogy, the Commerce Department's ITA has been for decades applying a legally sound *de jure* and *de facto* analysis to identify control and affiliation among foreign enterprises. Companies may either be legally (*de jure*) controlled by their government or may be affiliated with their government or other companies through facts and circumstances (*de facto*).

By way of example to illustrate, typically under trade laws, 25% legal ownership by a foreign government over a corporate entity amounts to *de jure* control, while 5% ownership amounts to affiliation. With respect to *de facto* affiliation, moreover, ITA typically looks to business relationships to determine whether there are sufficient mutual interests that could amount to control or influence by one business entity over another. Examples include close supplier/customer relationships or instances where companies are affiliated with one another through shared board members, shared management personnel, or family members.[14]

In fact, ITA's legal approach to control and affiliation is consistent with U.S. WTO obligations and has been upheld by U.S. tribunals, including the Court of International Trade and the Court of Appeals for the Federal Circuit. There is no reason why the same federal agency – the Commerce Department – cannot adopt this analysis for export controls. In fact, this more robust legal mechanism is needed to improve the effectiveness of the Entity List – i.e., by reducing the number of non-designated affiliates that could aid in the Entity List's circumvention. This legal approach would also enable the designation of Honor to the Entity List immediately. It is astounding that Honor, one of the principal entities that has been helping

---

[14] *See* 19 U.S.C. § 1677(33)(1994); 19 C.F.R. § 35l.102(b)(3).

Huawei circumvent the 2019 entity listing, has still not been designated to the Entity List four years later.

While it is true that BIS does not have the resources to identify and designate every affiliated entity to the Entity List, this is not what is required. The Commerce Department could share the burden with the U.S. exporters seeking licenses to potential affiliates. More specifically, BIS could designate to the Entity List as many subsidiaries and affiliates as possible using the *de jure* ownership analysis similar to that of ITA, *i.e.*, 25% ownership or more would amount to control, and 5% ownership or more would be affiliation. With respect to the more complex *de facto* affiliation analysis, however, BIS would take a different approach. It would issue regulations that automatically designate affiliates to the Entity List without expressly naming each one. The effect of BIS's regulations would be to put exporters on notice that they now need to conduct their own due diligence to ensure that they are not violating Entity List designations (much like the due diligence conducted to identify parties related to those on the Specially Designated Nationals and Blocked Persons List administered by the Treasury Department).

Many exporters have sufficient market intelligence to ascertain, with a reasonable degree of confidence, whether the end user to which they seek to export has sufficient ties with the Entity Listed company such their relationship may amount to *de facto* affiliation. If exporters are uncertain, BIS could permit them to either obtain attestations/certifications from the end-user or the exporter can simply decide not to make the export.

To be clear, these broadened Entity List control/affiliation criteria would apply to only entities subject to the jurisdiction/control of foreign countries of concern. They would not apply to entities of allied nations that ought to benefit from a more flexible U.S. export control system.

3. Transparency in the Entity List Designation

Currently, the ERC is in charge of Entity List nominations and designations. Nominations are not made public, nor are records of ultimate decisions not to designate. The public only becomes aware of designations when they are announced and subsequently published in the EAR. Moreover, there is no timeline that governs the deliberations process, and designations may take up to a year or longer, even when important national security risks are at stake. This system needs to change to improve transparency, and the system should leverage greater stakeholder input.[15]

It is important that the ERC obtain information from the private sector and other federal agencies for its Entity List designations, and so the ERC needs to create a new process to enable meaningful stakeholder input. The process should allow members of the public as well as U.S. Government bodies to submit nominations for the Entity List. Consistent with the low legal threshold for designations to the Entity List, moreover, nominations need not be accompanied by actual proof of wrongdoing but only the basis by which the submitters have "reasonable cause to believe, based on specific and articulable facts" that the nominated entities have "been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States."

Time limits are also important, so the ERC should establish a schedule for rendering final determinations, which could be extended on a case-by-case basis, and the ERC should make public all decisions not to designate specific entities. A public explanation not only improves transparency, but could also encourage other stakeholders to come forth with supplemental

---

[15] Transparency can be achieved without compromising sensitive classified U.S. Government information.

information that could prompt reconsideration of the nominee by the ERC. Whenever national security risks are at issue, reconsideration is entirely justified.

To maintain the integrity of this public nomination system, submitters should provide affidavits that certify the absence of conflicts of interest associated with their nominations.[16] The identities of the submitters should be kept confidential by the ERC, as retaliation by the PRC and other dangerous entities are becoming a real concern.[17] A carefully structured process, such as the one described here, is necessary to leverage greater stakeholder information to better safeguard U.S. national security and foreign policy interests.

E. License Standard: Presumption of Denial, Case-By-Case, and Presumption of Approval

Finally, BIS should assign to every entity on the Entity List a license review standard of "presumption of denial." There is no reason to review licenses to such entities through a less stringent standard, such as the "case-by-case" standard that applies to all other foreign recipients. Currently, there are hundreds entities on the Entity List, including Chinese and Russian entities that have a licensing review criteria of "case-by-case," and these include Huawei, Semiconductor Manufacturing International Corporation ("SMIC"), and Forensics Genomics International (a.k.a., BGI). There is one additional Chinese entity on the Entity List that has a license review criteria of "presumption of approval." That company is the Aviation Industry Corporation of China ("AVIC"), a PRC state-owned aerospace and defense conglomerate headquartered in

---

[16] For example, a submitter should state its ownership information, its affiliations, and interest in the Entity List designation.

[17] The identity of the submitter has no bearing on the ERC's evaluation of the factual contents of the nomination, which the ERC could corroborate through open-source information and/or internal Government records.

Beijing, which is the backbone of the country's military aviation industry.[18] This is absurd; there is no reason that a PRC military organization should fare better when designated to the Entity List than when not designated.[19]

F. License Review Policy for Exports to Foreign Countries of Concern

The PRC and other foreign countries of concern pose significant national security risks to the United States. As noted, the PRC, in particular, is undermining the peace and stability of the world order by threatening to harm the United States and its allies, and it is weaponizing American IP and technologies against the rest of the world. Despite this fact, the U.S. Government continues to adjudicate license requests to the PRC largely using a "case-by-case" review mechanism (except for specific end users and end uses). This is notwithstanding the PRC's Civil-Military Fusion strategy and the government's ultimate control over all PRC corporations through its range of national security laws. These laws compel the circumvention of U.S. export control laws in the PRC and facilitate the diversion of U.S.-controlled technology for dangerous end-uses to highly problematic end-users (including the military).

In light of these facts, BIS needs to review license requests for sensitive technologies to the PRC and other countries of concern under a license review policy of "presumption of denial." Albeit a very drastic approach, it is justified given that these malign governments are outrightly undermining global peace and threatening to harm the United States and its allies (or in some

---

[18] Amanda Lee, *Explainer | Chinese aviation firm Avic: why is it on a US sanctions list and what do we know about it?*, South China Morning Post (Mar. 28, 2021), https://www.scmp.com/economy/china-economy/article/3127089/chinese-aviation-firm-avic-why-it-us-sanctions-list-and-what.

[19] It should be noted that BIS maintains lists of dozens of companies that have been placed on the Entity List for surveillance activities associated with the forced labor camps in the PRC, including the drone company DJI, and tech companies Hikvision, IFLYTEK, etc. It defies reason that these companies would not be subject to sanctions under the Uyghur Human Rights Policy Act of 2020, as amended by the Uyghur Forced Labor Prevention Act, and the Global Magnitsky sanctions for their involvement in forced labor and other gross human rights violations.

cases, actually harming them). The U.S. Government's export control licensing policies should reflect these political realities. There is simply no other way to curb the misuse of sensitive, controlled U.S. technologies in these problematic countries. The U.S. Government has been attempting to find alternative solutions for decades but has failed.

G. Improvements to the De Minimis and Foreign Direct Product Rules ("FDPR"); Also See-Through Rule

The EAR's de minimis and FDP rules extend the extraterritorial coverage of the EAR to items produced abroad. Both rules, as they are currently written, do not adequately curb exports to foreign countries of concern.

1. Reducing the De Minimis Threshold for Countries of Concern

Under the EAR's *de minimis* rule, products manufactured abroad that incorporate greater than 25% U.S.-controlled content require a license prior to export (unless an exception applies). The *de minimis* rule is 25% for most countries, including the PRC, and it falls to 10% for Cuba, Iran, North Korea, and Syria. The *de minimis* threshold further falls to 0% for a very tiny group of items.[20] In light of the enormous national security risks posed by exports of sensitive goods, software, and technology to the PRC and other countries of concern, BIS should reduce the *de minimis* threshold for sensitive items to these specific countries.

2. Updates to the FDPR

The FDPR is a provision of the EAR that subjects items produced abroad to U.S. export license requirements when two narrow conditions are met. First, the foreign items must be the "direct product" of U.S.-origin technology or software controlled for very specific reasons, and

---

[20] Bureau of Industrial Security, *De minimis Rules and Guidelines*, (Nov. 5, 2019), https://www.bis.doc.gov/index.php/documents/pdfs/1382-de-minimis-guidance/file.

the foreign-produced item must also be subject to very specific controls if it were in the United States. The narrow scope of specific controls required to effectuate this rule makes it too limited. Additionally, the technology/software must also require a written assurance from the foreign recipient as supporting documentation for an export license (unless an exception applies). For example, semiconductor chips produced abroad from a very narrow list of controlled software/technology would be subject to controls if the chips themselves also fell within a narrow band of controls (i.e., a small subset of ECCNs) if located within the United States.[21] Second, a foreign-produced item meets the scope of the rule if it is destined for a country listed in Country Groups D:1, E:1, or E:2 of the EAR, which includes the PRC and Russia.[22]

To underscore, the FDPR does not adequately restrict exports to these group of countries, given the fact that it applies to only a very narrow subset of ECCNs and only under certain conditions. For exports to foreign countries of concern, BIS should consider expanding the EAR's FDPR control requirements to capture a broader group of ECCNs. That is to say, any item produced abroad from software/technology that are controlled for a broad range of reasons should be subject to the EAR's license requirement if the product would also be controlled for any reason if produced in the United States. This is somewhat analogous to the broad Huawei FDPR and should be applied to foreign exports to PRC entities and entities located in all other countries of concern.

---

[21] The foreign-made product would also be covered if made by a foreign plant or if it is a major component of a plant which itself is a direct product of U.S.-origin software or technology and which requires a written assurance. Plus, the foreign-made product must itself be subject to NS controls if produced in the United States.

[22] 15 C.F.R. § 734.9 (2023); supplement no.1 to part 740 of the EAR.

3. The EAR Needs A See-Through ITAR Equivalent Rule

The EAR also needs to better regulate exports of sensitive, controlled items when they are embedded in finished goods or subcomponents, whether produced domestically or abroad and destined to foreign countries of concern. The shortcoming may be characterized as follows: if a gaming computer containing highly-sensitive semiconductors is exported from the United States to PRC, it does not require an export license if the gaming computer itself is not subject to the CCL and is not destined to prohibited end-users or for prohibited end uses. The PRC's re-exports of the gaming computer to Russia would similarly not be regulated under the EAR. This gap permits the exports of sensitive semiconductor chips without licenses when embedded into another product (or without the appropriate licenses if the final exported product is subject to lower controls than the embedded chips).

The ITAR works far better than the EAR in these circumstances because it has a "see through" rule that attaches controls to an item, whether or not embedded within another product. In other words, ITAR controls do not disappear simply because the article subject to the USML is integrated into another item. Specifically, when an ITAR-controlled defense article is integrated into a larger system or end-item, the article does not lose its identity and is normally subject to its own license requirement. In other words, the ITAR "sees through" the larger system/end items and continues to regulate embedded defense articles. The same concept is needed in the EAR to better regulate exports to foreign entities of concern.

H. Disputes in License Adjudication Process and Escalation Procedures

Currently, export licenses under the EAR are adjudicated by bureaus within the Departments of Defense, State, Commerce, and Energy. Should these agencies disagree on an export license decision, the disagreement may be escalated to the export control "Operating

Committee" and subsequently to the Advisory Committee on Export Policy ("ACEP") led by BIS's Assistant Secretary for Export Administration (it excludes the Assistant Secretary for Export Enforcement). BIS's Assistant Secretary may override other agencies' votes, such that the adjudication process could become imbalanced.

There is no reason that BIS's Assistant Secretary needs to lead the dispute resolution; this process ought to be revised by giving lead authority to BIS's Under Secretary, who is better able to take into account the diverging views of BIS's Assistant Secretaries for Export Enforcement and Export Administration. Moreover, BIS's authority to overrule other agency votes needs to change as well. Each agency must have one equal vote, and if a licensing dispute remains unresolved through a tie, the final tie-breaking decision must be made by the National Security Council.

I. Improvements to the End-Use Check System

The integrity of the U.S. export control system can only be validated through adequate end-use checks of foreign entities. End-use checks are routinely conducted to detect misuse of controlled goods, software, or technology by the foreign recipient, and they are also conducted to ensure that unauthorized entities do not have access to controlled items. Yet, end-use checks are weak and ineffective in the PRC and non-existent in other foreign countries of concern. In the PRC specifically, the Ministry of Commerce ("MOFCOM") severely impedes end-use checks by BIS officials. By contrast, MOFCOM does allow comprehensive audits by Commerce Department ITA officials for trade remedy cases. There is no rational justification for MOFCOM's different treatment of these two Commerce Department bureaus unless, of course, MOFCOM's intent is to obfuscate information relating to the PRC's export control violations.

For context, when BIS issues export licenses, the licenses generally outline the terms and conditions associated with the U.S. Government's export authorizations. Consequently, the foreign end users must adhere to BIS's terms and conditions and cannot, for example, reexport the item to an embargoed country or to a prohibited end user (e.g., Russian Military) without a license. Similarly, they may not transfer the product in-country to an unauthorized recipient (e.g., another entity or an Entity Listed company) without a license. Yet, with very severely constrained end-use check capabilities in the PRC, which last only a few hours and are closely regulated by the PRC government, U.S. officials are unable to adequately probe the records of their targets to detect violations.

Until the PRC government allows Commerce Department BIS officials to conduct robust end-use checks and at the frequency they desire, BIS ought to deny export licenses to the PRC. It defies logic that the U.S. Government would want to authorize exports of sensitive items to the countries that impede BIS's ability to validate their proper end use. Furthermore, in light of the PRC's national security laws and anti-foreign sanctions laws that demand that PRC entities disregard and evade U.S. export controls requirements and, given the PRC's extensive history of export control violations and diversion to Russian, North Koran, and Iranian entities, this recommendation makes sense. Until the Commerce Department is allowed to conduct full, robust, complete, and unencumbered end-use checks by the PRC government and until it is satisfied that the PRC's diversion practices have ceased, BIS cannot license <u>any</u> exports of sensitive controlled items to the country.

The Commerce Department should also strengthen the <u>forensic</u> audit capabilities of its Export Enforcement officers through improved and frequent training so they are able to better detect export control violations. Additionally, much like ITA's audit reports of foreign

producers/exporters subject to trade remedy cases, BIS end-use check officials should also publish reports of its end-use checks. These reports can be made public with specific confidential, business proprietary information redacted (but not for Congressional oversight committees). Redactions must be made sparingly so that the public may review and provide input on the integrity of the end-use check methods and the veracity of the foreign entity's representations. There is no reason to keep such critical information regarding important national security interests confidential when public versions can readily be made.

J. Controlling Exports of Critical Technology Through Universities to Foreign Countries of Concern: The Fundamental Research Exception

The most talented scientists in the United States are researching critical emerging technologies at major universities funded by taxpayer dollars, yet the EAR's fundamental research exception allows such research to fall outside of the jurisdiction of export controls when "intended" for publication.[23]

Fundamental research under the EAR specifically means "research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons."[24] According to the EAR:

> "Technology" or "software" that arises during, or results from, fundamental research and is intended to be published is not subject to the EAR.
>
> Technology" or "software" that arises during, or results, from fundamental research is intended to be published to the extent that the researchers are free to publish the "technology" or "software" contained in the research without restriction. "Technology" or "software" that arises during or results from

---

23 15 C.F.R. 734.8(a) (2016).

24 *Id.*

> fundamental research subject to prepublication review is still intended to be published when:
>
> (1) Prepublication review is conducted solely to ensure that publication would not compromise patent rights, so long as the review causes no more than a temporary delay in publication of the research results;
>
> (2) Prepublication review is conducted by a sponsor of research solely to insure that the publication would not inadvertently divulge proprietary information that the sponsor has furnished to the researchers; or
>
> (3) With respect to research conducted by scientists or engineers working for a Federal agency or a Federally Funded Research and Development Center (FFRDC), the review is conducted within any appropriate system devised by the agency or the FFRDC to control the release of information by such scientists and engineers.

In short, this rule makes clear that America's most sensitive research may be exported to foreign adversaries (including through deemed exports) whether the results of the research are intended to be published broadly.

This rule is fundamentally flawed in that it fails to consider risks associated with the foreign talent recruitment programs of many adversary countries. Further, the mere possibility that technologies may be published sometime in the future is not sufficient reason for exempting these technologies from control today. At present, sensitive weapons, supercomputer, biotechnology, and semiconductor research are occurring at U.S. universities with participation by PRC students that are part of the countries' Thousand Talents program. Even when foreign students are not aligned with their government at the time of study in the United States, they may be coerced by their government to return home (or threatened to return) with the technology that the government seeks to obtains and ultimately uses for malign purposes. This is a real risk when dealing with countries of concern that have programs in place that are specifically designed to exploit these gaps in our laws.

In this context, it becomes clear that the definition of fundamental research needs to be strengthened to better prevent exports of sensitive technologies to adversaries. With respect to any research at American universities that pertain to or draws upon technologies currently controlled on the CCL, the fundamental research exception should be removed for countries of concern.

K. Sensitive Technology, When Published, Is Not Subject to the EAR

Generally, when controlled technology or software is published in a public forum,[25] it is exempt from export control under the EAR. According to the EAR, information and "software" are not subject to controls when they are, *inter alia*, published,[26] or released by instruction in a catalog course or associated teaching laboratory of an academic institution. This means that any entity may simply (sometimes temporarily) publish its most sensitive technology (*e.g.*, online) in order to circumvent export controls.

This rule is flawed, inconsistent with the ITAR,[27] and should be reformed. BIS should amend the EAR by prohibiting the publication of sensitive technologies – i.e., those that pose the highest national security risks – unless a license for publication is obtained first. BIS should endeavor to protect the circumvention of export controls, not enable it.

L. Gaps in October 7, 2022 Semiconductor Export Control Rules

On October 2022, the Department of Commerce issued a new set of export control restrictions intended to curb the PRC's semiconductor advancements. The October regulations

---

25 15 C.F.R. 734.3(b)(3) (1996).

26 As described in 15 C.F.R. § 734.7 (2020).

27 22 C.F.R. §120.11 (2022).

restricted – through export licenses – transfers of certain leading-edge ICs and chip technology, as well as certain semiconductor manufacturing equipment and services by U.S. persons involved in the development of leading-edge wafers within the PRC. The Government once again pursued "nuanced" regulations containing significant gaps that permit the legal transfer of equipment and technology to countries of concern. These include:

- Enabling Chinese firms operating in the PRC to re-incorporate outside of the PRC in order to sidestep restrictive export licensing requirements.
- Allowing foreign-produced items derived from U.S. controlled technology to reach specific, prohibited PRC entities on the U.S. Government's Entity List by diversion through other non-designated PRC companies.
- Limiting export controls on semiconductor manufacturing equipment to only ICs at leading-edge nodes (e.g., 14/16 nm and below for logic chips), ignoring the fact that most semiconductor equipment can be used to manufacture a range of leading-edge *and* advanced/legacy wafers with minor adjustments.
- Permitting U.S. persons to work in PRC chip plants and directly transfer expertise and know-how for advanced/legacy chips, even though their technology transfer may also indirectly (and substantially) impact the PRC's chipmaking capabilities at the leading-edge nodes, the level where the technology-transfer restrictions apply.

It may be the case that, in developing these new rules, the U.S. Government underestimated the PRC government's and the U.S. industry's motivations to exploit the gaps in the rules in order to "legally" bypass them. For the PRC government, its motivation, of course, comes from its quest to dominate the global semiconductor industry in order to grow its economic and military power.

For American businesses, on the other hand, the motivation is purely economic – they built substantial manufacturing capacity for the purpose of supplying the PRC market, and consequently, sales to the PRC are core to their business model. In fact, news reports have circulated about American and PRC semiconductor firms' assessments that their transactions

will not be materially curbed by the new export control rules. The U.S. Government itself has also encouraged exports of leading-edge ICs and technologies to the PRC by exempting semiconductor manufacturers from complying with the October rules for at least one year. In short, the new export control rules, as written and implemented, are weak and are unable to materially slow the PRC's growth in leading-edge IC design and production capabilities.

Further underscoring the problems with the new rules is the fact that they are shortsighted – by focusing restrictions on leading-edge IC capabilities, they do virtually nothing to address the PRC's massive wafer capacity expansion at the advanced/legacy node levels of 22 nm, 28 nm, 45 nm, and above. These nodes are the workhorses of the commercial and defense industrial base, powering consumer electronics, vehicles and transportation equipment, high-capacity energy storage systems, and weapons systems. Moreover, sales of advanced/legacy ICs account for the overwhelming majority of the global semiconductor manufacturing industry's annual revenue: approximately 95%. The United States needs to maintain a strong presence in this market segment because revenue from advanced/legacy chip sales directly funds next-generation leading-edge R&D designs and production capability.

Of course, the PRC government understands the strategic importance of these ICs and has dedicated hundreds of billions of dollars over the past several years to build massive advanced/legacy wafer fabrication facilities in the PRC that have already begun overproduction. As soon as these PRC-origin ICs flood the global markets and depress world prices, manufacturers in the United States, Taiwan, South Korea, and other allied nations will be squeezed out of the market – from both the advanced/legacy IC market segment as well as the ability to capitalize leading-edge IC innovations as well. The U.S. Government has not articulated any strategy to address this serious threat, and America's allies are similarly at risk.

Time is limited, and inaction is not an answer. The U.S. Government needs to close the gaps in its export control rules and further restrict exports of capabilities that are enabling the PRC's ongoing overcapacity efforts.

M. Further Tightening the EAR for Exports to Countries of Concern

Consistent with the foregoing, the U.S. Government needs a new Export Control Modernization effort to tighten EAR rules and policies governing licenses to countries of concern, including China and Russia (specifically, to revise/reverse the 2009-2016 policies). Key priorities for EAR modernization for countries of concern should be: (1) the elimination of the "specially designed" licensing loophole which currently allows exports of controlled technologies to foreign adversaries,[28] and (2) the tightening of deemed export rules to mirror the ITAR.[29]

---

[28] Specially designed" is a description often used for specific items listed on the CCL. Generally, it is a technique that ***excludes*** items from export controls – i.e., it is the "release" part of BIS's "catch and release" export licensing scheme. When an item is "specially designed" for a controlled purpose, that essentially means in BIS parlance that the item has "properties peculiarly responsible for achieving or exceeding the performance levels, characteristics, or functions in the relevant" export control category. In other words, if the item can operate at that specified performance level *and below*, for example, and when designing the product the engineer contemplated that the item would operate at that performance level and below, then the item is likely not "specially designed" and hence not controlled under the relevant ECCN. Note that this is a very flexible standard and can be used to exclude many critical items from the control category. In reality, there is no need to have this definition. If an item is not specially designed for a particular performance level but can nonetheless perform at the controlled level, it needs to be regulated through export controls. No exception, no "release."

[29] The ITAR defines an export to a foreign person, whether or not in the United States, as follows: "any release in the United States of technical data to a foreign person is deemed to be an export to all countries in which the foreign person has held or holds citizenship or holds permanent residency as defined by 22 C.F.R. § 120.50." The ITAR defines a foreign person as "any natural person who is not a lawful permanent resident as defined by 8 U.S.C. § 1101(a)(2) or who is not a protected individual as defined by 8 U.S.C. § 1324b(a)(3)." The EAR defines exports to a foreign person as follows: "any release in the United States of 'technology' or source code to a foreign person is a deemed export to the foreign person's most recent country of citizenship or permanent residency." 19 C.F.R. § 734.13. A foreign person, moreover, is defined by the EAR as "any natural person who is not a lawful permanent resident of the United States, a citizen of the United States, or any other protected individual as defined by 8 U.S.C. 1324b(a)(3). In other words, the ITAR evaluates a foreign person based on all countries where the person currently holds or has held citizenship, or holds permanent residency, where the EAR only

Additionally, under the EAR, when a specific type of technology is available abroad, BIS tends either to NOT to control it or BIS approves license requests to export the U.S.-origin technology abroad. That is the "foreign availability" policy.[30] But foreign availability does not mean foreign willingness to sell. Also, many times, products that are available abroad are very distinguishable in terms of quality and performance levels such that the restriction of a U.S. export would be effective in that it would compel an adversary to source a lower performing "foreign available" product.

The extent to which BIS performs these types of analyses and renders conclusions as to why it has found certain products to be available abroad (resulting in a license approval to an adversary) and why it has found certain products to not be available abroad (resulting in a license denial to an adversary), it should make the public on a quarterly basis. Again, confidential data about the U.S. exporter, foreign country of concern end user, any other party involved in the transaction or proprietary quantity and value data may be kept confidential. However, basic comparisons of products need not be kept confidential and should be made public to improve transparency over export controls. Given that the scope of this recommendation is limited to exports of foreign countries of concern, it stands to reason that Congress and the American public would want increased transparency.

looks to the foreign person's most recent country of citizenship or permanent residency. Moreover, EAR deemed export rules come into play only if a person discloses any development, production, or "use" technology related to the controlled product to a foreign person. Here, the problem is that the term "use" requires the inclusion of operation, installation, maintenance, repair, overhaul, and refurbishing information, such that if one of these are eliminated, the deemed export rule does not apply.

[30] Pursuant to the EAR, "foreign availability exists when the Secretary determines that an item is comparable in quality to an item subject to U.S. national security export controls, and is available-in-fact to a country, from a non-U.S. source, in sufficient quantities to render the U.S. export control of that item or the denial of a license ineffective." 15 C.F.R. § 768.2 (a).

N. Rebutting Arguments Against Restricting Exports of Sensitive Items to the PRC

Finally, it is worth underscoring that the two main policy arguments traditionally advanced by the U.S. industry to advocate against restrictive export control rules are misplaced and need to be summarily rejected. The first argument erroneously stipulates that highly restrictive controls on exports to the PRC will compel American firms to relocate abroad in order to avoid regulation. This is an outdated argument and ignores the reality of today's economic order. Presently and for the foreseeable future, there is simply no country in the world that would offer the same business environment as the United States in terms of regulatory transparency, intellectual property protection, economic stability, and infrastructure. Furthermore, conditions in the Indo-Pacific region are becoming increasingly unstable as escalating aggressions by the PRC and North Korea threaten neighboring countries. Europe, for its part, is dealing with a historical energy crisis that is not expected to subside in the near- and medium-term. And other allies in South America and globally have not yet developed the skilled workforce needed to support the U.S. semiconductor industry's demands. To be sure, there is no better place to invest, operate, and innovate than the United States – even when stringent export control rules are in place.

The second argument is similarly misguided in that it posits that the U.S. semiconductor industry desperately needs revenue from the PRC in order to grow. This argument misses the fact that it is enormously risky to become financially dependent on an adversary while also building the adversary's capabilities through technology transfer. Contrary to the flawed premise of this argument, access to the Chinese market is not a zero-sum game, and sales revenue may indeed be generated elsewhere. In fact, the U.S. semiconductor industry can (and should) diversify away from the PRC by building a resilient supply chain at home and further

supporting the development of a complementary ecosystem in the countries of its neighbors and allies. Even though creating an alternative supply chain is not easy and will take time to develop national security and economic security imperatives demand the reorientation of the industry towards a robust, reliable, and stable ex-PRC trading ecosystem system. America stands to lose too much if the current trajectory continues.

IV. CONCLUSION

I would like to conclude with one final note. The world is edging towards an unprecedented national security crisis that may reshape the world order in the long term against U.S. interests. The adversary, the PRC and other foreign countries of concern have been emboldened by U.S. transfers of technology, knowhow, assets, and capital for years, and led by the PRC, they are now strong enough to seriously harm America's allies and pull the United States into a global conflict. In order for the United States to lead and defend our allies, we must improve our ability to strategize offensively and defensively, and among the most important strategies is the protection of our most critical technological assets. America needs to protect its technologies in order to rebuild at home and reclaim its technological lead over the PRC. Again, the PRC has the workforce, the capital, and the capability to sprint ahead of the United States. We should not strengthen the PRC's hand by transferring more technology to them. Our vulnerabilities are currently significant, and we need to focus internally rather than on exports to malign actors. Time is not on our side, and the challenge ahead of us is enormous.

Appendix

May 11, 2022

Statement of Hon. Nazak Nikakhtar

Partner, International Trade and National Security Practice Chair, Wiley Rein LLP
Former Assistant Secretary for Industry & Analysis, Under Secretary for Industry & Security*
U.S. Department of Commerce

Testimony Before the Senate Select Committee on Intelligence*

Threats to U.S. National Security:
Countering the PRC's Economic and Technological Plan for Dominance

Senator Warner and Senator Rubio, Committee experts, policy advisors, and staff, thank you for the opportunity to speak about the growing challenges posed by the People's Republic of China ("PRC") to U.S. and global national security and economic security interests, and the appropriate U.S. Government response.

My name is Nazak Nikakhtar, and it is an honor to appear before you today. I am an international trade attorney and Chair of the National Security practice at the Washington, DC, law firm of Wiley Rein LLP. I am also a trade and industry economist, a former Georgetown University adjunct law professor, and recently completed my second tour of duty in the U.S. Government. Twenty years ago, I began my career as an analyst at the Department of Commerce's Bureau of Industry and Security and subsequently at the International Trade Administration, where my colleagues and I witnessed from the frontlines the predatory economic tactics used by our trading partners to erode our industries. In 2004, I helped establish and lead the Commerce Department's China/Non-Market Economy Office and, for several years thereafter, I audited numerous foreign (including Chinese) companies and their affiliates for the Department. In 2018, I returned to the Commerce Department to serve as Assistant Secretary for Industry & Analysis and, in 2019, I simultaneously served, performing the non-exclusive functions and duties, as the

**Performing the non-exclusive functions and duties of Under Secretary while also serving as Assistant Secretary.*

The views and opinions expressed in this testimony are mine only and do not represent the views of Wiley Rein LLP or any of the firm's clients.

Under Secretary for the Bureau of Industry and Security. It is from all of these vantage points that I offer my testimony and observations today about the risks to U.S. national and economic security, as well as the gaps in U.S. laws that must be closed to adequately mitigate these risks. There are many.

I. THE EROSION OF SUPPLY CHAINS AND THE RESULTING ECONOMIC AND NATIONAL SECURITY THREATS

Only recently, in 2017, the U.S. Government began to aggressively confront the challenges posed by the PRC's predatory economic practices. These challenges had been ignored for decades and, as a result, over the course of the past 40-plus years, the United States continuously lost capabilities in sector after sector in manufacturing, technology, and services that are essential to our national security. In goods alone, the offshoring of manufacturing has created supply chain vulnerabilities across hundreds of critical products, ranging from semiconductor and electronics manufacturing to the development of active pharmaceutical ingredients. This has led to job losses of between 3.4 to 3.7 million between 2001 to 2018.[1] In key sectors such as communications equipment, electronics, and computer technology, we ceded up to 40% to 60% of the domestic market share to Chinese imports, and globally the PRC has captured extensive market shares in those sectors as well.

Let me be clear on two key points. First, these are not incidental consequences of open and free trade. These are the very perverse and adverse consequences of one country exploiting open borders to cripple other nations' economies. Our economic losses have resulted from the PRC's deliberate attempts to hollow out our industries in order to create dependency on their own

[1] Robert Scott and Zane Mokhiber, *Growing China Trade Deficit Cost 3.7 Million American Jobs Between 2001 and 2018*, Economic Policy Institute (Jan. 30, 2020), available at https://www.epi.org/publication/growing-china-trade-deficits-costs-us-jobs/.

distorted market. The weaker our industries become – semiconductors, telecommunications, critical minerals and rare earth elements, high-capacity batteries, and pharmaceuticals and medical equipment – the more our national security is at risk.[2] Without access to secure supply chains, we are unable to sustain our economies, and we are unable to develop the weapon systems necessary for national defense. The result is that our military will have a "one strike" capability. This is also true for our allies and the rest of the world.

Second, the economic facts before us should make abundantly clear that the PRC government has waged an economic war against the rest of the world aimed at eroding non-Chinese supply chains so that no country is able to depend on itself or its allies for the essential items it needs. The PRC's end game is to render the rest of the world dependent on it, and today this plan is succeeding. At present, we depend on the PRC for 80% of our critical minerals,[3] 20-23% of our semiconductor chips (92% on Taiwan for our most advanced chips),[4] 60% of our consumer electronics including telecommunications equipment,[5] 75% of our lithium-ion battery cells,[6] and 100% for many of our pharmaceuticals and medical supplies. The greater our dependence grows, the more vulnerable and fragile we become. This is not a sound strategy.

---

[2] President Biden's 2021 supply chain Executive Order lists these critical sectors. *Executive Order on America's Supply Chains*, The White House (Feb. 24, 2021), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.

[3] *A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals*, U.S. Department of Commerce (2019), available at https://www.commerce.gov/sites/default/files/2020-01/Critical_Minerals_Strategy_Final.pdf.

[4] *Strengthening the Global Semiconductor Supply Chain in an Uncertain Era*, Boston Consulting Group and Semiconductor Industry Association (Apr. 2021) at 5, 35, available at https://www.semiconductors.org/wp-content/uploads/2021/05/BCG-x-SIA-Strengthening-the-Global-Semiconductor-Value-Chain-April-2021_1.pdf ("BCG/SIA 2021 Report"); *Taking Stock of China's Semiconductor Industry*, Semiconductor Industry Association (July 13, 2021), available at https://www.semiconductors.org/taking-stock-of-chinas-semiconductor-industry/.

[5] BCG/SIA 2021 Report at 28.

[6] Gavin Thompson, *Batteries with Chinese Characteristics*, Wood Mackenzie (Feb. 10, 2021), available at https://www.woodmac.com/news/opinion/batteries-with-chinese-characteristics/; *Protecting Americans' Sensitive Data From Foreign Adversaries, Exec. Order No. 14034 of June 9, 2021*, 86 Fed. Reg. 31,423 (June 11, 2021), available at https://www.govinfo.gov/content/pkg/FR-2021-06-11/pdf/2021-12506.pdf.

To be clear, we have not yet felt the full adverse effect the PRC's control over our supply chains and economies yet. Not because control does not exist, but rather because the PRC government has chosen not to exercise it yet. When will that time come? When the PRC knows that we are too weak to respond – perhaps when it displaces the U.S. dollar from the global currency market, or when it fully indigenizes leading-edge semiconductor development such that it no longer needs U.S. technology. This time horizon is only a few years away. This is becoming an immediate threat.

As a nation, we tend to downplay these risks because we steadfastly hold onto the belief that the United States' economy is strong and resilient, and so it will be immune from external threats. The prevailing argument – that U.S. purchasing power will continue to keep the PRC dependent on the United States and prevent it from harming U.S. interests – is terribly misinformed. We source from the PRC not because we choose to but because we have little other option. Today's economic reality is that United States and the rest of the world have absolutely no choice but to import heavily from the PRC because this is where supply chains for the most critical products reside. The current trade deficit with the PRC, which stood at $355.3 billion in 2021, underscores this point.[7] The coronavirus pandemic highlighted supply chain reality. And the farther our supply chains migrate into the PRC, the greater our dependence will become.

As our import dependence on PRC-origin goods expands, we need consider the following question: Will the PRC government guarantee to the rest of the world fair and equitable access to its supply chains? The answer is a definitive "NO." We have already witnessed instances of the PRC's stranglehold over its trading partners. For example, the debt-trap deliberately created by

---

[7] The deficit with China increased $45.0 billion to $355.3 billion in 2021. Exports increased $26.6 billion to $151.1 billion and imports increased $71.6 billion to $506.4 billion. *U.S. International Trade in Goods and Services, December 2021*, U.S. Department of Commerce Bureau of Economic Analysis (Feb. 8, 2022), available at https://www.bea.gov/news/2022/us-international-trade-goods-and-services-december-2021.

the PRC's One Belt One Road scheme where African and South American countries, who were once lured by the PRC government's promises for substantial investment, have now been forced to give up their most valuable national assets (*e.g.*, mines, roads, and ports) in repayment.[8] These countries are now at the PRC government's mercy and, so far, their only recourse is to ask the United States and other countries for assistance. We – the United States, our North America allies, European and Asian partners – are all nearing this dangerous tipping point as well.

For those of us who have studied the PRC in-depth for decades, this is precisely the PRC government's end game: to deplete other nations of the resources necessary for self-defense by creating supply chain weaknesses and economic dependence. This PRC strategy, coupled with reports of the PRC government's endless intimidation of Taiwan, Japan, Australia, South Korea, and Lithuania, and the government's repeated threats of military attacks against the United States and its allies must make absolutely clear that we are not dealing with a friendly nation. The PRC government is a threat, and both the Trump and Biden Administrations have designated the PRC government as a "foreign adversary" along with the governments of the Republic of Cuba, the Islamic Republic of Iran, the Democratic People's Republic of Korea, the Russian Federation, and Venezuela's Nicolás Maduro Regime.[9] This designation means something.

To be clear, the United States, Europe, and the rest of the world are already in a very vulnerable position with respect to critical minerals and semiconductors supply chains. Without access to these goods, we have very little leverage over the PRC government, and our military capabilities are severely limited. This, then, leads to the obvious question: if the PRC government

---

[8] Jeremy Mark, *China's Real 'Debt Trap' Threat*, Atlantic Council (Dec. 13, 2021), available at https://www.atlanticcouncil.org/blogs/new-atlanticist/chinas-real-debt-trap-threat/.

[9] *Securing the Information and Communications Technology and Services Supply Chain*, 86 Fed. Reg. 4,909, 4,911 (Dep't Commerce Jan. 12, 2021), available at https://www.govinfo.gov/content/pkg/FR-2021-01-19/pdf/2021-01234.pdf.

were to restrict global access to its critical mineral exports, as well as its own and Taiwan's semiconductor supply chains, what would be the economic impact and how would we respond?

The economic impact to the United States will be in the trillions. Compounded by the economic impact across the rest of the world – the result will be catastrophic. Almost everything we manufacture or consume today, and all of our technological advancements, depend in some way on Chinese-processed critical minerals or Chinese and Taiwanese semiconductor supply chains. Without access to these materials, the global economy will come to an abrupt halt.

As to how we would respond, our response would be ineffective. Realistically, it will take a minimum of three to five years to scale production of critical minerals mining, extraction, and processing capabilities to wean dependence off the PRC. Additionally, it will take at least 10 to 20 years to recreate the vast semiconductor ecosystem that currently exists in the PRC and Taiwan, including the development of upstream raw material and chemical supply chains, as well as the back end assembly/testing/packaging capabilities, which are presently concentrated in the PRC and Taiwan.[10] During this transition period, our countries are vulnerable.

This is the point that most policymakers fail to realize. The PRC is leveraging its near monopoly over critical global supply chains to secure its ambitions for economic and military hegemony. We need to quickly reverse our vulnerabilities, and I urge the Commission and Congress to act before it becomes too late.

II. THE UNITED STATES MUST RETHINK ITS APPROACH TO NATIONAL SECURITY AND TRADE LAWS

For years, I have described the predatory economic tactics that the PRC government has systematically used to weaken our industries and economy, and I have often stressed that we do

[10] BCG/SIA 2021 Report at 19.

not adequately leverage our laws to counter these security threats. Appended hereto is my prior testimony on this topic. Today, however, my goal is to offer perspectives on how to cure our vulnerabilities in order to better protect our economies and technologies. The recommendations I provide may not all be easy. They will require sacrifices. But if we, as a nation, are resolute, we may be able to solve our weaknesses before it is too late.

Success will depend on open trade and reliance on the comparative advantages of the United States and our allies. Success will depend on our ability to work together to reconfigure supply chains out of the PRC. And success will depend on forging greater economic ties between like-minded partner countries. For the United States, the economic impact of moving our supply chains out of the PRC is approximately 1% of U.S. gross domestic product in the short-run. If we do this in concert with our European, Japanese, and South Korean allies, the economic impact is significantly lessened. After three to five years, any negative economic impact will turn into substantial gains for the United States and those gains will grow significantly. Overall, the benefit to the free world of disentangling from a predatory actor will be immeasurable.

A. Deterring Invasion of Taiwan

At the outset, one of the most immediate threats to global security is the PRC government's potential move on Taiwan, whether by military force, legal decree, or another mechanism. The PRC government's objective in obtaining control over Taiwan is to gain control over the island's semiconductor and electronics industries, and thereby gain almost absolute control over the global economy. In other words, control over Taiwan will allow the PRC government to bring the global economy to its knees.

Importantly, however, the United States still controls one of the most powerful weapons of the global economic order – the U.S. dollar. The dollar's special status as the global currency gives our nation unrivaled sanctioning power. Given that access to dollars is a near-necessity for

multinational businesses and global financial institutions, the United States is able to impose significant economic damage by denying certain entities or governments access to the dollar. Indeed, the sanctions that are currently pummeling the Russian currency, banks, and the internal economy are a vivid demonstration of the power of the U.S. dollar. Coupled with sweeping European sanctions, the United States and its allies are capable of imposing significant costs to the PRC economy through comprehensive financial sanctions on PRC banks should it take control of Taiwan.

It should be noted that the PRC government is now hastening efforts to reduce reliance on the U.S. dollar to protect itself from potential U.S. sanctions. It is simultaneously working to displace the dollar from serving as the global currency in favor of the Yuan. But it will take years for the Yuan to gain any significant foothold in the global economy. Until then, and while the dollar still maintains substantial influence, the U.S. Government should be prepared to use this economic lever as deterrence.

B. The U.S. Government Needs A Legal Mechanism to Recognize PRC Entities' Ties to the Central Government

Over the course of the past 10 years, the PRC government has steadily increased its control over Chinese companies. And by doing so, it has coerced companies to aid the central government in growing its military base, technological capabilities, and surveillance activities. It is well documented that the PRC government mandates and coerces – through law, administrative guidelines, and regulations – entities to transfer sensitive information, trade secrets, and intelligence information to the central government. In addition, PRC laws require that entities conform their practices to advance the Chinese Communist Party's ("CCP") military and

surveillance interests.[11] Moreover, the PRC's Military-Civil Fusion strategy demands that entities cooperate with the People's Liberation Army ("PLA") to advance the military strength and ambitions of the PRC government for global power. All Chinese entities, even those enterprises that still remain ostensibly private and civilian, are legally obligated to serve the state and the leadership of the central government such that Chinese entities have limited autonomy over their business decisions. The PRC government's routine installation of CCP officials inside private firms ensures compliance with the party's mandates.

The reality today is that Chinese entities operate in a military-driven ecosystem that is centrally coordinated by the CCP to advance the country's weapons capabilities, intelligence operations, and security apparatuses. The legal framework through which the PRC government forces entities to contribute to the modernization and expansion of the CCP's military industrial complex continues to expand rapidly and, therefore, poses a significant threat to the national security, foreign policy, and economy of the United States.

In light of the foregoing, it is surprising that the U.S. Government does not have a consistent legal framework across all federal agencies for finding affiliation between Chinese commercial entities and the PRC central government. In fact, it never has. Crippled by this lack of comprehensive legal framework, the U.S. intelligence community has been hampered in both its offensive and defensive capabilities, the U.S. Department of Defense is limited in the types of companies it can eliminate from supply contracts, and U.S. Government agencies are unable to

---

[11] USCBC, *Fact Sheet: Communist Party Groups in Foreign Companies in China*, China Business Review (May 31, 2018), available at https://www.chinabusinessreview.com/fact-sheet-communist-party-groups-in-foreign-companies-in-china/.

legally prohibit procurement from CCP affiliates or prohibit U.S. investments in PLA affiliates.[12] However, if the U.S. Government had an actual legal framework to determine whether companies are (1) controlled by the PRC government, or (2) affiliated with the PRC government, it could do more to protect U.S. industries, economy, and national security from their malign activities.

Accordingly, U.S. Government should develop a comprehensive, consistent, and complementary legal standard for evaluating the extent to which commercial and non-commercial PRC entities are controlled by or affiliated with their provincial or central governments. The lack of framework has, to date, significantly impeded the U.S. Government's analysis in export controls, foreign direct investment screenings (discussed further below), intelligence community risk assessments, federal government acquisitions, and supply chain vulnerability analyses. This shortcoming ought to be remedied, and the solution is quite simple. Congress should, by legislation, adopt the longstanding legal definitions of affiliation that exist in U.S. trade laws, through statute, regulations, and case precedent, and apply these definitions to augment the legal authorities currently existing across all federal agencies. The trade laws extend the definition of affiliation beyond ownership interests to the broad range of ways in which foreign governments are able to exercise influence over corporate entities' business operations such that the entities lose autonomy over key decisions. These trade laws have been upheld by U.S. courts for decades, are consistent with the United States' obligations under the World Trade Organization ("WTO") agreements, and will therefore withstand judicial scrutiny. It is axiomatic that the application of a comprehensive legal standard such as this would improve each federal agency's ability to maximize the use of its own existing authorities where a determination of affiliation is needed.

---

[12] *E.g.*, through the U.S. Department of the Treasury's Chinese Military Industrial Complex companies. *See Non-SDN Chinese Military-Industrial Complex Companies List (NS-CMIC List)*, U.S. Department of the Treasury (Dec. 16, 2021), available at https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/ns-cmic-list.

Further, a consistent legal approach such as this would promote uniformity and predictability across the U.S. Government agencies' legal authorities and provide better clarity to businesses seeking regulatory approvals from various agencies.

C. The United States and Its Allies Should Rely More Heavily on Export Controls

The PRC's growth has been driven in significant part by U.S. companies as well as firms in allied nations racing to transfer technology to Chinese counterparts – many of which are controlled by the PRC government – in exchange for temporary access to the PRC market. The fact that the PRC government restricts access to its domestic market in exchange for technology transfer to individual companies confirms the extensive collusion and connection between PRC companies and their central government.

This technology-transfer trend has accelerated over the course of the past two decades and has resulted in so much technology transfer to the PRC that the PRC is now technologically neck-in-neck with the United States in many important sectors (*e.g.*, telecommunications and computers), and vastly ahead in others (*e.g.*, hypersonic weapons, artificial intelligence, genomics, and robotics). This is incredibly alarming. In order to solve this problem, we need to revise our current strategy.

1. The Need for a "Block" and "Run Faster" Approach

At the outset, the United States' export control community has traditionally pursued a competition strategy of "run faster" when it comes to developing export control policies.[13] The theory behind this strategy is that, by permitting exports of critical technologies to PRC entities, U.S. firms will gain access to the revenue needed in order to invest in next-generation technologies and stay ahead in the technology race. But this strategy has failed over the years. Although it

[13] It is important to emphasize that export controls are not prohibitions on exports per se. They simply subject exports to a license review process.

takes our firms years, even decades, to develop new technologies, we are handing over these technologies to the PRC virtually overnight, allowing them to bypass the extended technology-development lead times and costs (including trial-and-error) that innovators endure. In other words, our strategy has been to place the painstaking technology development burden on our own businesses, and then allow the rapid transfer of the resulting technology to adversaries enabling them to "run faster" than us. Two examples demonstrate the danger of the 'tech transfer for revenue' approach.

ASML is the Dutch photolithography company that developed the highly-advanced and one-of-a-kind extreme ultraviolet ("EUV") lithography tool that produces the most leading edge semiconductors in existence today. This tool was developed, in part, using U.S.-controlled technology. ASML is the only firm in the world that is capable of making these sophisticated machines,[14] and it has taken ASML 20 years to develop this tool with billions of dollars in investments.[15] If the PRC semiconductor industry were to acquire this machine, it would be able to reverse engineer it in three years, giving it a substantial boost in semiconductor development and solidify its position as a global leader. Indeed, the PRC semiconductor industry in 2020 surpassed Taiwan for the second year in a row in global semiconductor chip sales.[16] With this added EUV capability, along with the downstream assembly/packaging/testing ecosystem that the

---

[14] Sam Shead, *Investors are Going Wild Over a Dutch Chip Firm, And You've Probably Never Heard of It*, CNBC (Nov. 24, 2021), available at https://www.cnbc.com/2021/11/24/asml-the-biggest-company-in-europe-youve-probably-never-heard-of.html.

[15] Matthew Gooding, *ASML Might Be The Most Successful Tech Company You've Never Heard Of*, Tech Monitor (Aug. 6, 2021), available at https://techmonitor.ai/technology/future-of-asml-photolithography-semiconductor-chip-euv.

[16] *China's Share of Global Chip Sales Now Surpasses Taiwan's, Closing In on Europe's and Japan's*, Semiconductor Industry Association (Jan. 10, 2022), available at https://www.semiconductors.org/chinas-share-of-global-chip-sales-now-surpasses-taiwan-closing-in-on-europe-and-japan/.

PRC government has developed, the PRC will be positioned to dominate the global chip industry likely by 2025.[17]

In comparison, the United States is lagging behind; we do not have the capability to produce all of the semiconductors required for our defense capabilities, let alone a substantial portion of our economy. We produce neither all of the upstream raw materials necessary to manufacture the chips, nor do we maintain an assembly/packaging/testing ecosystem to operationalize the chips. This is the fundamental problem. It will take 10 to 20 years to rebuild an on-shore and complementary near-shore semiconductor ecosystem to cure the United States' and our allies' dependence on the PRC and Taiwan. The PRC, by contrast, is only a few years away from independence.

The second example is the well documented PLA's advancements in hypersonic weapons, which was facilitated by the transfer of U.S. semiconductor technology to the PRC. To be clear, one U.S. company's technology transfer allowed the PRC military to race ahead of the United States, and that company's realized short-term profits now threatens our national security and the world's security.

Clearly, we need a different strategy – one that both blocks technology transfer and allows us to run faster. This means that we need more aggressive export controls on transfers of critical technology through the denial of export licenses to adversaries in the PRC. We also need to augment investments in U.S. innovation, as discussed further below.

---

[17] Tim De Chant, *The Chip Choke Point*, The Wire China (Feb. 7, 2021), available at https://www.euvlitho.com/Blogs/The%20Chip%20Choke%20Point%20-%20The%20Wire%20China.pdf; Robert Castellano, *3 Headwinds Facing ASML's Non-EUV Business in China*, Seeking Alpha (Mar. 22, 2021), available at https://seekingalpha.com/article/4415477-three-headwinds-facing-asml-s-non-euv-business-in-china, Misha Lu, *Is Huawei Making its Own Lithography Equipment*, Tech Taiwan (June 9, 2021), available at https://techtaiwan.com/20210609/huawei-duv/.

2. Controls on Emerging Technologies

Although the Export Control Reform Act of 2018 ("ECRA") legislated the protection of "emerging technologies" through the use of export controls,[18] the debate continues in the U.S. Government as to the most effective way to implement ECRA's mandates and restrict such exports. At the outset, there is widespread recognition that emerging technologies are most vulnerable to foreign acquisition when they are at the nascent stages of development. Congress recognized this reality when it used the term "emerging" in ECRA. Indeed, at the nascent stage of development, the full range of applications that may arise from new technologies are seldom identified. Because Congress recognized this uncertainty, it instituted regulatory controls over their exports given that the same technologies that wield the power to drive significant advancements in the commercial sector may also be exploited for both known and yet-to-be known dangerous uses by foreign adversaries. Artificial Intelligence is a perfect example of this intersection.

My understanding is that the U.S. Government appreciates the enormous difficulty associated with the task of identifying "emerging technologies" for export controls when those technologies and their applications are constantly evolving. The Government further recognizes that, in order to move forward with controls, it must decide between two very different types of regulatory approaches. The first option is to wait until "emerging" technologies develop into somewhat better understood, more "mature" technologies in order to be more precisely defined for controls (in much the same way that most technologies are identified on export control lists). Alternatively, the U.S. Government has the option of acting more swiftly by delineating and controlling broader categories of technologies as "emerging technologies" under ECRA.

---

[18] Export Control Reform Act, H.R. 5040, 115th Cong. § 106 (2018).

I do not believe that the U.S. Government has abandoned either option to date, even though there are downsides associated with each. The former approach, whereby "emerging technologies" are narrowly defined, risks additional delay in instituting controls that are presently needed. Moreover, by attempting to define technologies that are not yet fully understood with a high degree of specificity, the Government may inadvertently omit necessary technologies from control. A too-narrow definition also increases the likelihood of circumvention by technology developers who may be able to reconfigure their technologies in minor ways in order "design out" from the scope of controls. On the other hand, the alternative approach of adopting a broader definition of "emerging technologies" – while it allows for the more expeditious implementation of licensing requirements – runs the risk of regulating more exports than necessary to protect national security. To the extent the U.S. Government adopts either option, it should consider imposing licensing requirements for only exports of emerging technologies to entities and/or countries that pose the most significant national security risks. To the extent that the acquisition of emerging technologies by U.S. allies does not pose risks, allies could be exempt from licensing requirements. This approach additionally eases the licensing burden on federal agencies and U.S. businesses.

3. Exports to Countries that Do Not Permit Adequate End-Use Checks

The U.S. Government also needs to better control technology transfers to countries with inadequate "End-Use Checks," like the PRC. End-use checks are mechanisms by which U.S. Government officials conduct on-site audits of foreign recipients' ("end users") use of controlled items to determine whether the items are being used in accordance with the terms and conditions associated with the U.S. Government's export authorization.

Today, in order for the U.S. Government to conduct an end-use check of any PRC entity, it must notify the PRC government of its intent and seek the government's authorization in advance

of the actual check. Often, end-use checks are not permitted for weeks. This affords the PRC government ample time to tamper with the end user's records in order to obfuscate any evidence of export control violations. The PRC government and its companies are notorious for falsifying records and diverting exports of controlled items to unauthorized end users within the PRC (*e.g.*, the PLA, military end users) and countries abroad (*e.g.*, Iran). The U.S. Government needs to take this reality into account.

If the U.S. Government does not have full confidence in its ability to conduct thorough and transparent end-use checks in the PRC, then it should not authorize exports of sensitive items to the PRC at all. At a minimum, the Government ought to adjudicate export licenses to the PRC under a "presumption of denial" evaluation criteria rather than the current "case-by-case" criteria, which is normally enjoyed by firms in nations that authorize end-use checks by U.S. officials and otherwise fully comply with U.S. export laws. The PRC should not be subject to the same license review criteria as fully-cooperating partners. This policy needs to change.

4. Entity List License Review Criteria

The U.S. Government should also update its Entity List policy. The Entity List (found in Supplement No. 4 to Part 744 of the Export Administration Regulations ("EAR")[19]) "identifies entities for which there is reasonable cause to believe, based on specific and articulable facts, that the entities have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United

[19] 15 C.F.R. § 744.16, available at https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744/appendix-Supplement%20No.%204%20to%20Part%20744.

States."[20] Where the U.S. Government determines that reasonable cause exists, it may include a parent company, as well as its affiliates, on the Entity List.[21]

For items subject to the EAR, the entity listed companies are generally prohibited from receiving U.S. exports absence a license from the U.S. Commerce Department, and the majority of export licenses to Entity List companies are subject to a "presumption of denial" license review policy. The legal threshold for including entities on the Entity List is by design a flexible standard so that the U.S. Government has improved ability to curtail these entities' harmful actions through export licenses.[22]

Today, there are a number of entities on the Entity List where U.S. exports are subject to an export license review policy of "case-by-case" or "presumption of approval," rather than the "presumption of denial" policy. These more lenient license review criteria obviate the punitive impact of a company's designation on the Entity List. It makes no sense to place a PRC entity on the Entity List for having engaged in malign activities if, through the designation, the entity is able to benefit from the same or better export-license adjudication procedures than non-harmful actors.

Congress has, in the past, requested license review and approval statistics for PRC companies on the Entity List and has been surprised by the large number of export licenses approvals to Entity Listed companies. This is the reason.

---

[20] *Clarification of Entity List Requirements for Listed Entities When Acting as a Party to the Transaction Under the Export Administration Regulations (EAR)*, 85 Fed. Reg. 51,335 (Bureau of Indus. and Sec. Aug. 20, 2020), available at https://www.govinfo.gov/content/pkg/FR-2020-08-20/pdf/2020-17908.pdf.

[21] 15 C.F.R. § 744.11(b).

[22] Company-specific Entity Listings are not a substitute for item-specific export controls. An Entity Listing regulates exports of many items to a specific entity (*e.g.*, SMIC, Huawei), whereas the control list designation regulates exports of a particular item to all entities in various countries. These authorities are not substitutes and should not be used interchangeably.

5. Unilateral Versus Multilateral Controls

It is also worth pointing out that the notion of consistently favoring a multilateral approach for export controls over a unilateral approach may not always be justified and may ultimately impede the implementation of much-needed controls to safeguard national security. The reality is that not all countries are able to move in lock-step with the United States by imposing controls at the same speed, same scope, same manner, and at the exact same time.

Most countries' economic exposure to the PRC and geopolitical vulnerabilities are far greater than the United States', and these exposures necessitate a different approach to controls. For example, Europe is far more economically entangled with the PRC, and South Korea and Japan are far more geographically vulnerable. In light of this reality, it makes little sense for the U.S. Government to continuously demand multilateral export restrictions and expect allies to consistently act in unison in order for it (the U.S. Government) to act. Again, this delays the implementation of controls to protect U.S. national security.

Where the United States has the will and ability to impose controls in advance of its allies, it should do so and with faith that our allies will likely follow our lead. This is exactly what happened when the United States imposed restrictions on U.S. exports to Chinese telecom giant Huawei Technologies Co., Ltd. ("Huawei") several years ago. Had the U.S. Government pursued export restrictions multilaterally, the restrictions would never have been imposed.

For reference, in May 2019, the United States placed Huawei on the Entity List for its violation of U.S. financial sanctions against Iran.[23] The U.S. business community responded with outrage because it argued that foreign countries would increase sales to Huawei and displace U.S.

---

[23] *Addition of Entities to the Entity List*, 84 Fed. Reg. 22,961 (Bureau of Indus. and Sec. May 21, 2019), available at https://www.govinfo.gov/content/pkg/FR-2019-05-21/pdf/2019-10616.pdf.

business opportunities. Businesses, in effect, complained that America's allies would work against U.S. interests. But that is not what happened. In fact, the exact opposite occurred.

Soon after the U.S. Government placed Huawei on the Entity List and restricted exports to Huawei under a "presumption of denial" export license review policy,[24] America's allies began pulling back sales to Huawei. Not because they were legally obligated to do so, but because it was the correct course of action. Yet they did not pull back publicly. Each country, given its own unique economic and political circumstance, retreated from Huawei in its own manner, most often quietly and without any public fanfare. In fact, the United States' unilateral action caused a multilateral ripple effect among our allies, and by our giving them "top cover," our allies followed suit. The result, of course, was the crushing defeat of Huawei's smartphone business.[25]

This example illustrates that, when coordinating export controls with allies, we need not always move in in perfect synchronicity. The United States should, whenever necessary, act to protect its national security interests and be assured that our allies will follow, albeit at their own pace and through their own legal mechanisms.

6. Closing the Fundamental Research Gap in Export Controls

Further, our adversaries are exploiting research in our universities to obtain cutting-edge technology, and our universities are in turn freely transferring technology to high-threat actors using the "fundamental research" exception of the export control rules. The EAR currently defines fundamental research as:

---

[24] The license review policy was subsequently changed in August 2020 to a "case-by-case" license review criteria for most exports.

[25] Rob Thubron, *Huawei experiences largest-ever revenue fall as sanctions crush its consumer division*, Tech Spot (Aug. 6, 2021), available at https://www.techspot.com/news/90696-huawei-sees-largest-ever-revenue-fall-sanctions-crush.html.

> {R}esearch in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons.[26]
>
> "Technology" or "software" that arises during, or results from, fundamental research and is intended to be published is not subject to the EAR.[27]

These exceptions permit the flow of cutting-edge research and development in critical technologies – for example, artificial intelligence ("AI"), leading edge semiconductor design and production, lithium-ion batteries, robotics, genomics – to high-threat actors. This is another gaping hole in our laws that needs to be closed.

U.S. universities ought to be subject to export control licensing requirements before engaging in such technology transfer, and there are steps that the U.S. Government can take to regulate this flow of information. An immediate step is to issue notices to universities (via a Presidential Proclamation or a Federal Register notice) providing that licenses would be required for sharing controlled technology with non-U.S. persons. The legal mechanism here is the "is-informed" process, which is a "stop gap" measure where the U.S. Government informs the entity/entities (universities in this case) of a license requirement in advance of a formal rule change. Subsequently, the U.S. Government should revise its definition of "fundamental research" in the EAR to make it more restrictive. Fundamental research should be treated no differently than controlled technology; once basic research evolves into the type of know-how matching control levels, licenses should be required. Indeed, the U.S. Government maintains the authority to change its own regulations to keep pace with new national security threats. It must do so now; time is overdue.

---

[26] 15 C.F.R. § 734.8.

[27] *Id.*

7. Export Controls on Data

In today's high-technology ecosystem, there is no reason why we are not controlling through export controls data transfers to foreign adversaries, especially when it is public knowledge that our data are being used and misused by our adversaries to build dangerous AI capabilities and massive surveillance machines. Similarly, U.S. businesses should not be placing data storage centers in the countries of our adversaries or allowing them to have any control over our domestic data storage systems. Some of these transactions would never come under the review of the Committee on Foreign Investment in the United States ("CFIUS") (falling below the regulatory thresholds or developments through greenfield investments), so we need independent legal authority to deal with this risk. The proposed outbound investment review legislation discussed below would help regulate the transfer of data storage centers abroad. Export controls are additionally needed to regulate the export of sensitive data.

8. Secondary Sanctions as a Tool

Secondary sanctions should also be leveraged as a viable economic tool. The U.S. Government and Congress receive substantial information on a regular basis – whether through intelligence reporting or public news outlets – of sanctions violations by PRC entities. Under U.S. laws, violations of U.S. sanctions are punishable by the imposition of secondary sanctions. Yet, the U.S. Government has, to date, been reluctant to punish PRC companies for such violations. Presumably, the reason for this is the extent of American companies' financial exposure to the PRC.

Herein lies the irony of the U.S. Government's policies. The U.S. Government, on one hand, is unable to hold PRC entities accountable for undermining U.S. national security interests and, on the other hand, permits businesses to transact with harmful entities even though doing so

fuels the PRC's growth. Our refusal to impose secondary sanctions also emboldens PRC entities to continue undermining U.S. interests.

Our policies need to change. Secondary sanctions need to be used to address activities that undermine U.S. national security interests.

9. Revenue Substitution – Away from the PRC and Towards Allies

Finally, we should dispel the prevailing notion that U.S. businesses need revenue from sales to the PRC in order to invest in next-generation technologies and survive economic competition. Indeed, any revenue lost from sales to the PRC may be replaced (and even augmented) by increasing sales within the United States and to nations of allies. It makes no sense to invest in the supply chains of an adversary instead of our own. We must build our own supply chains, as well as our allies', in order to achieve much-needed redundancies in our most critical supply lines. Furthermore, redundancy is essential where supply chains are most vulnerable. The U.S. Government should support investments to build supply chains domestically and with allies.

D. Regulating Foreign Direct Investment ("FDI") Flows

The U.S. Government needs to better regulate FDI flows that harm U.S. economic and national security interests.

1. Delayed Reviews of FDI in Existing Critical Technology Businesses

The Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA") represented a major milestone in protecting national security by granting to CFIUS enhanced authority to protect "critical technologies" from foreign acquisition through FDIs. However, nearly four years into its enactment, the U.S. Government has not yet been able to fully utilize this new authority. This is because FIRRMA's definition of "critical technologies" rests in large part on ECRA's identification of "emerging technologies," and until the U.S. Government makes progress on this issue, gaps in our national security laws persist.

Here too, the question of whether to narrowly or broadly define "emerging technologies" (as explained above) has important implications in the context of reviews of FDI transactions. On one hand, a broader definition would subject a wider range of transactions to FIRRMA authority, thereby giving the U.S. Government increased visibility into U.S. FDI activities and greater authority to restrict those that threaten national security. On the other hand, it is argued that increased regulatory oversight will deter FDI flows into the United States. To address this latter concern, the U.S. Government could consider limiting mandatory filing requirements to only those entities and/or countries that pose the most significant threats to U.S. national security. This would decrease regulatory burdens on U.S. businesses and ultimately reduce the volume of transactions subject to review by federal agencies. A broader definition applied to a narrow set of countries is the most effective and efficient national security approach.

Whichever option the U.S. Government pursues has serious implications. But the ultimate point here is that the U.S. Government needs to make substantial progress in its identification of "emerging technologies" under ECRA and "critical technologies" under FIRRMA. Movement on these fronts will give businesses some clarity going forward and enable the U.S. Government to better exercise the legal authorities it possesses to protect national security. The exercise of those authorities has, for nearly four years, languished.

2. Merits of Outbound Investment Reviews

In much the same way that FIRRMA and its predecessor, the Foreign Investment and National Security Act of 2007, imposed national security reviews on inbound FDI transactions, Congress is now considering similar legislation for outbound investments to high-risk countries. New legislation would call for CFIUS-type reviews of U.S. asset flows to foreign markets for national security risks. Even though this outbound investment review screening mechanism is one

of the most important pieces of legislation before Congress today, it is one of the most contentious.[28]

To the extent there is any question as to whether such investment review mechanisms are warranted, we should be clear about how urgent the situation has become. At the end of 2020, U.S. investments in in PRC companies totaled by capital investment type (public and private equity):

- U.S. Entity List Companies: $48.6 Billion
- PRC State-Owned Enterprises: $152 Billion
- PRC Military End User and Chinese Military Companies: $54 Billion
- Telecommunications: $43 Billion
- Robotics: $1.3 Billion
- Biotechnology: $50.4 Billion
- Artificial Intelligence: $221 Billion
- Surveillance: $3.8 Billion
- Aerospace and Defense: $1.3 Billion
- Semiconductors: $21 Billion
- Pharmaceuticals: $31 Billion

In total, U.S. financial investments in Chinese domiciled companies totaled over $2.3 trillion in market value of holdings at the end of 2020. Compounding this fact is the additional transfer of our technology and supply chains, and the outbound investment screening legislation is a key step to solving this problem. We need this law.

Before I explain the merits of this proposed legislation, it is important to level-set, as there has been extensive misinformation about this law. The proposed legislation is not in any way an

[28] To lessen the burden on U.S. businesses in filing notices of such transactions for federal agency review and to ease the workload for U.S. Government agencies adjudicating such transactions, the scope of reviews could be limited to outbound transactions involving foreign countries that pose the most significant national security threats.

overreach by Congress to interfere in the free market – far from it. Rather, the proposed legislation is essential to protecting U.S. national security interests that are currently unprotected. To be clear, businesses are primarily motived by revenue, and that is their strong suit. Yet, this fact should not cause them to be unregulated, especially when profit seeking interests undermine U.S. national security. It is the Government, not business, that is charged with protecting national security, and to the extent transactions strengthen adversaries in dangerous ways, the Government must intervene. We have, for centuries, regulated the transfer of defense articles to foreign adversaries. Today, in much the same way, we need to regulate the transfer of technology, economic flows, and supply chain capabilities to them. These are the new weapons of modern economic warfare and our strategic capabilities should not fall into the wrong hands.

As a nation, we need to come to terms in particular with our technology transfer to the PRC. Make no mistake, the PLA's hypersonics advancements were fueled by U.S. chip technology. One company's short-term profits have now threatened to erode the United States' and the world's national security and economic stability. That makes no sense. Our data and technology transfer have also enabled the PRC to race ahead with AI, where reports are starting to surface that Chinese enterprises are using our software and phone apps to track and monitor our movement and behavior data.

As Joseph Stalin is rumored to have said: "We will hang the capitalists with the rope they sell us." Whether this quote is accurate or not, it is illustrative of what is happening today. We have had decades of unregulated supply chain and technology transfer to the PRC that has systematically eroded our own supply chains and rendered us dangerously dependent on the adversary. This is not a good national security strategy. We need a new strategy.

As I mentioned, there is currently no legal authority that reviews these types of transactions for national security risks – namely, joint ventures between U.S. and foreign firms abroad, the acquisition by U.S. firms of shares in companies abroad, or the transfer of a skilled work-force abroad. Such business transactions are frequent and, in the countries of foreign adversaries where the government regularly coerces businesses to act in ways that undermine U.S. national security interests, the risks are serious.

There are four key ways that business transactions are able to undermine U.S. national security interests by transferring to the foreign country/business the following:

(1) transfer of emerging uncontrolled technology,

(2) transfer of operational know-how that may fall below export controls but nevertheless confers critical know-how to build and/or operate very sensitive machinery (e.g., for nuclear reactors),

(3) transfer of engineers that will develop technologies abroad and so will fall outside the jurisdiction of U.S. export controls (this also results in a "brain drain" in the United States), and

(4) movement of critical manufacturing capabilities and supply chains abroad, such as lithium-ion batteries, active pharmaceutical ingredients, semiconductor manufacturing operations, and medical supplies including personal protective equipment ("PPE").

The foregoing should illustrate that this is a zero sum game; our adversaries' gain is our loss, and our gain is their loss. We need to be clear about this reality. The more we invest in a government-run, command-style non-market economy that is designed to undermine our markets, the more we move production to the PRC to avail ourselves of its cheap prices, forced labor, and other non-market distortions, and the more we purchase cheap goods from PRC businesses rather than goods produced in market economies, the more we allow non-market forces to capture a greater share of the global market. In this way, we are accelerating the demise of capitalism and the market based system. We need outbound review and restrictions as a measure to protect

national security. That is Congress's responsibility and I commend you for not losing sight of this objective. Congress should pass this legislation as it is a national security imperative.

3. Reconsidering CFIUS Mitigation Agreements with the PRC

The U.S. Government's CFIUS "mitigation agreement" policy also warrants reconsideration in light of the PRC government's laws mandating that Chinese and foreign companies transfer sensitive intellectual property, proprietary commercial secrets, and personal data to the central government and the PLA. Among the relevant PRC laws are:

- **National Security/Intelligence Laws:** mandating the transfer of data, information, and technology to the PRC authorities.[29]
- **Cybersecurity Law:** mandating that network operators cooperate with public security organs. [30]
- **Cryptography Law:** eliminating "core function exemption" for products with encryption as general features. [31]
- **Data Security Law:** empowering CCP authorities to demand data from companies and requires companies to "favor economic and social development in line with the CCP's social morality and ethics." [32]
- **Export Control Law:** prohibiting exports of "important data," essentially any information outside of China, even if that data originated from a foreign country, including a U.S. business.[33]

These laws appear to apply to all companies operating in the PRC, regardless of nationality and, in some instances, they also appear to have extraterritorial application, reaching to corporate

---

[29] *Data Security Business Advisory: Risks and Considerations for Business Using Data Services and Equipment from Firms Linked to the People's Republic of China*, U.S. Department of Homeland Security (Dec. 22, 2020) at 6-7 ("DHS Advisory"), available at https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

[30] Lauren Maranto, *Who Benefits from China's Cybersecurity Laws?*, Center for Strategic & International Studies (June 25, 2020), available at https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws.

[31] DHS Advisory at 8-9.

[32] *Id.* at 7-8.

[33] Ck Tan, *China's Export Control Law to Become 'Key Dynamic' in U.S. Relations*, Nikkei Asia (Dec. 1, 2020), available at https://asia.nikkei.com/Economy/China-s-export-control-law-to-become-key-dynamic-in-US-relations.

operations abroad. In the CFIUS context, these laws likely trump the U.S. Government's mitigation agreements.

In reviewing transactions for national security risks, CFIUS commonly enters into agreements with parties in order to mitigate any national security risk resulting from the transfer of information, data, or technologies from the United States to the foreign acquirer. However, when the foreign acquiror is a PRC entity that is also subject to its own governments' data transfer requirements, that entity cannot logically be expected to abide by both the U.S. mitigation agreement and the conflicting PRC government laws. In other words, when a conflict exists between CFIUS's prohibitions on information transfer and the PRC's mandate for data transfer, there is simply no way to adhere to both requirements.

Of course, the PRC government has levers to compel cooperation with its own laws instead of the United States' requirements. One example is the PRC government's nationwide social credit rating system that applies to all corporations for the purposes of detecting misconduct and non-compliance with PRC government rules.[34] The "Corporate Social Credit System" has implications for companies with respect to proprietary technical information, sensitive personal data, and surveillance information. Companies may be given low scores if they fail to transfer their data to the PRC government as part of their obligations. Failing to score well, by non-compliance with the PRC government's policies or demands, may subject companies to myriad sanctions, including higher taxes or permit difficulties, or a blacklisting which could mean financial ruin for that entity.

---

[34] *See, e.g.*, *China's Corporate Social Credit System*, Congressional Research Service (Jan. 17, 2020), available at https://crsreports.congress.gov/product/pdf/IF/IF11342; Kendra Schaefer, *China's Corporate Social Credit System: Context, Competition, Technology and Geopolitics*, Trivium China (Nov. 16, 2020), available at https://www.uscc.gov/sites/default/files/2020-12/Chinas_Corporate_Social_Credit_System.pdf.

The European Chamber of Commerce describes this credit rating system as potentially amounting to "life or death" for companies.[35]

The U.S. Government and Congress must account for the PRC's enormous control over companies and evaluate the effectiveness of the CFIUS agreements. Until the U.S. Government is able to resolve the conflicts described above, it should not permit mitigation agreements for any PRC transactions.

4. The Need for National Security Reviews of Greenfield Investments

Unregulated greenfield investments in the United States also pose very real risks to our national security interests. While CFIUS jurisdiction currently extends to certain real estate transactions that are located within certain geographical areas, for example, certain pre-defined military installations,[36] "greenfield" investments are not broadly subject to CFIUS jurisdiction. This is an enormous gap in our regulations.

Today, malign actors are able to acquire real estate in the United States and use this asset to harm the U.S. interests in a variety of significant ways. Examples include (1) the disruption of regional economic commerce by interfering with critical supply chains (*e.g.*, agriculture, transportation, telecommunication); (2) the displacement of U.S. manufacturers through economic distortive trade activities (underpricing or overproduction to eliminate competition); (3) the acquisition of sensitive personally identifiable information about the general population (*e.g.*, genetic, biometric data); (4) the use of soft power and political propaganda to undermine U.S. democracy (*e.g.*, political promotion programs and media); (5) mass surveillance of U.S.

---

[35] *European Chamber Report on China's Corporate Social Credit System, A Wake-Up Call for European Businesses in China*, European Chamber of Commerce (Aug. 28, 2019), available at https://www.europeanchamber.com.cn/en/press-releases/3045/european_chamber_report_on_china_s_corporate_social_credit_system_a_wake_up_call_for_european_business_in_chin.

[36] 31 C.F.R. §§ 800.213, 802.212.

populations (through the establishment of hotels, medical, and service oriented businesses); and (6) the disruption of the energy grid through the transmission of malicious code (*e.g.*, through malicious software in electric vehicle charging stations or smart homes that connect to the grid). These are just a few examples.

President Biden has already warned the American public that the PRC government has been conducting large-scale cyberattacks against the United States.[37] Indeed, some of these threat vectors are coming from within our own boarders. In 2014, the China Rail Rolling Stock Corp. ("CRRC"), a PRC state-owned enterprise, built a passenger rail assembly plant in Springfield, Massachusetts. Over time, this investment destroyed U.S. competition in the rail car market. The CRRC now has passenger rail cars in the U.S. North East, Midwest, and West Coast and it is able to leverage these assets to conduct massive surveillance operations over major U.S. populations and control the movement of the public. Presently, the CRRC controls more than 83% of the global rail market, and the company has publicized its aim to dominate the remainder of the world market as well.[38]

Of course, FDI is capable of delivering enormous benefits to an economy. But the U.S. Government must be aware of the risks posed by malign investors as well. The time is ripe to expand CFIUS jurisdiction to greenfield investments. Even though the U.S. Government will never be able to entirely eliminate all threat vectors from its borders, it must do a better job of addressing the range of threats that exist right now.

---

[37] Sean Keene, *Biden Administration Blames China For Microsoft Exchange Email Hack*, C Net News (July 19, 2021), available at https://www.cnet.com/news/privacy/biden-administration-blames-china-for-microsoft-server-hack/.

[38] David C. Lester, *Rail Security Alliance Expresses Concern about CRRC to U.S. Dept. of Defense*, RT&S (June 9, 2021), available at https://www.rtands.com/passenger/rail-security-alliance-expresses-concern-about-crrc-to-u-s-dept-of-defense/.

E. The Chips Act

The Chips Act is a crucial first step to growing the domestic semiconductor manufacturing base in order for the United States to become self-sufficient in semiconductor manufacturing capability and the associated intellectual property. The majority of this capability currently resides in the PRC, Taiwan, and Southeast Asia. Presently, there are quite a number of rumors concerning potential beneficiaries of the Chips Act using financial awards to not only invest in U.S. manufacturing facilities, but also to funnel the corporate capital otherwise saved to investments in China and other geographically vulnerable regions in Southeast Asia. This is an enormous problem. The Chips Act is necessary to strengthen U.S. supply chains and thereby avoid risks associated with our adversaries' growing stranglehold over this sector. It would be antithesis to the object and purpose of the Act to fund domestic industries while allowing the same beneficiaries to double-down on Chinese investments and undermine U.S. national security. There ought to be guardrails put in place in any forthcoming appropriations language.

Further, lawmakers should be mindful of the fact that creating a resilient U.S. supply chain for chips is a an enormously complex endeavor, as secure supply chains outside of the PRC and Southeast Asia are needed for a range of semiconductors products (e.g., logic, memory, analog, digital, and mixed-signal) at varying nodes (180 nm, 7 nm, 5 nm, etc.). In total, this comprises hundreds and thousands of discrete semiconductor chip types with unique chip designs. Additionally, investments are also needed for the development of next-generation lithography technology to manufacture leading edge chips in the United States. As the PRC is endeavoring to acquire current technologies, we need to stay steps ahead.

Moreover, we need to build resilient supply chains for the backend and highly-technical assembly, packaging, and testing capabilities. We also cannot lose sight of the upstream supply chains required to manufacture both the semiconductor chips and the wafer fabrication

equipment themselves, including as raw materials certain critical minerals (e.g., gallium, germanium), chemicals (e.g, hydrofluoric acid), superabrasives (e.g., diamond powder), etc. Most of these supply chains – for both the United States and our allies – reside in the PRC and Southeast Asia.

Finally, the U.S. military needs to ensure that we have robust domestic capabilities – from raw materials, wafer fabrication equipment, to backend assembly, testing, and packaging – to manufacture the semiconductors needed for defense applications, in the event that access to the South China Sea is blocked and armed conflict ensues. Without a strong upstream and downstream military supply chain, our armed forces will only have one-strike capabilities. This is a dangerous position to be in.

F. Trade Remedy Laws Must Be Improved to Protect Injured U.S. Industries

Substantial improvements must also be made to existing U.S. trade remedy laws to better protect injured U.S. industries and provide American businesses with the support needed to re-grow.

1. The PRC's Distortion of the Surrogate Country and Surrogate Value Methodology

From the early 2000s, following the China's 2001 accession to the WTO, the PRC government began an aggressive push to erode U.S. industries through predatory pricing practices. Trade with the PRC increased over the years, and the number of trade disputes grew exponentially.

Presently, the United States has over 223 trade remedy cases against the PRC versus a total of 441 cases against all other nations combined.[39] This is astounding, and the level of harm inflicted by PRC exporters through their underpricing behavior is the most significant of any other

[39] United States International Trade Commission Website, available at https://www.usitc.gov/.

trading nation. What is more, the number of complaints against the PRC continues to increase well into the its third decade of WTO accession. This tells us something very important: that the PRC is continuing to take advantage of the multilateral trading system in order to displace competitors from the global market.

While the United States currently maintains a robust set of trade remedy laws (antidumping and countervailing duty laws) to offset unfair trade and "level the playing field" for domestic manufacturers, many of the policies that the U.S. Government pursues to carry out these laws need to be updated to address the PRC's growth.

One of the most compelling areas for change is the manner in which the U.S. Government selects "surrogate" countries in dumping proceedings to value goods produced by the PRC. Because the PRC is a non-market economy, the U.S. Government relies on third country prices, or "surrogate country" prices to value the cost of production in the PRC (which is then compared to U.S. prices to measure unfair dumping). However, because PRC goods have penetrated global markets so aggressively, it is nearly impossible to find a surrogate country that has not been adversely affected by the PRC's predatory pricing. Prices around the world have been depressed so extensively that virtually all benchmark prices in trade cases are now understated and inadequate for measuring underselling by the PRC.

The result is that the tariffs ultimately imposed by the U.S. Government on Chinese imports to offset dumping are inadequate to "level the playing field," and consequently proper relief is denied to American firms. The U.S. Government must update its tools to more effectively prevent harms to the domestic industry. The present system is failing.

2. Section 301 Investigations to Address Additional Predatory Economic Practices and Creation of An Innovation Fund

Finally, Section 301 of the Trade Act of 1974, as amended, provides a remedy against country-specific unfair trade practices, and action is permissible if the United States Trade Representative determines that U.S. rights under a trade agreement are being denied, or a practice by a foreign country violates or is inconsistent with a trade agreement, or is unjustifiable and burdens or restricts U.S. commerce.[40] If such a finding is made, Section 301 authorizes the U.S. Government impose a range of remedial trade measures, including but not limited to the imposition of tariffs on goods imported from the foreign country.

It has been rumored that the United States may be considering, in addition to the current Section 301 tariffs on PRC goods for intellectual property theft (*i.e.*, tariffs ranging from 7.5% to 25% on specific imports),[41] tariffs in response to the PRC government's use of industrial subsidies. That is, a new Section 301 investigation would be launched to determine whether such industrial subsidies have harmed U.S. interests.

Beyond IP theft and industrial subsidies, there are numerous additional ways in which the PRC is undermining U.S. national security and economic security interests. The PRC focuses on areas where existing laws are inadequate or altogether nonexistent: global overcapacity, covert cyberattacks, market access restrictions (in China), and the exploitation of assets in the U.S. market.[42] Here too, USTR should conduct Section 301 investigations on these practices and

---

[40] Section 301 of the Trade Act of 1974, as amended (19 U.S.C. § 2411).

[41] Section 301 tariffs were imposed by the United States on imports from the PRC to recoup the approximately $50 billion a year economic harm to the U.S. economy caused by the PRC's intellectual property theft. *See Section 301 Tariffs on Goods from China: International and Domestic Legal Challenges*, Congressional Research Service (April 5, 2022), available at https://crsreports.congress.gov/product/pdf/LSB/LSB10553.

[42] For example, PRC entities underselling through physical presence in the U.S. market where existing trade remedy tools that are specific to countering unfairly priced imports (e.g., antidumping and countervailing duty laws) would not apply, and where Federal Trade Commission anticompetition laws do not probe national security threats for action.

impose import-restrictive measures to recoup the value of economic harm caused to U.S. businesses.

Moreover, if affirmative determinations of harm are made as a result of the Section 301 investigations and additional Section 301 tariffs are imposed on imports, then the U.S. Government should consider shifting the tariff payment responsibility onto PRC exporters rather than U.S. importers. Currently, U.S. Customs and Border Protection requires that the "importer of record" (which may be the U.S. importer or foreign exporter) pay tariffs on imported goods. However, often for the payment of Section 301 tariffs, PRC exporters pressure U.S. importers to bear the costs. If, however, the responsibility for the Section 301 tariffs were legally placed on the PRC exporter, it would relieve the U.S. importer of this financial burden. Through a Presidential Proclamation, the U.S. Government could legally require PRC exporters to be liable for 301 tariffs.

Furthermore, the U.S. Government should consider using the tariff revenue collected to create an "Innovation Fund" dedicated to capitalizing high-technology U.S. industries. The fund should ideally be used to assist U.S. manufacturers and innovators, including high-end semiconductor technology companies and infrastructure companies, obtain a strong foothold in the U.S. market through augmented research and development investments and facility builds. The U.S. Government has collected well over $100 billion in Section 301 tariffs since their original imposition in 2018, and these tariffs, in addition to any new ones, should be directed at growing and catalyzing U.S. innovation and industry growth. The revenue stream certainly exists, and so the U.S. Government should leverage this opportunity to support the nation's industrial and engineering advancements.

III. CONCLUSION

I would like to conclude with a one final note. The world may very well be on the brink a new national security crisis. In order for the United States to lead and defend our nation and our allies, we must have a robust economy, a strong manufacturing base, and the protection of critical assets and technologies. Our vulnerabilities are currently significant, and we need to quickly make important decisions to solve them. Time is not on our side and the challenge ahead of us is enormous.

I look forward to your questions.

ATTACHMENT

July 30, 2020

Statement of Nazak Nikakhtar
Assistant Secretary, International Trade Administration, Industry & Analysis
U.S. Department of Commerce

Before the
Senate Committee on Commerce, Science, and Transportation
Subcommittee on Security
"The China Challenge: Realignment of U.S. Economic Policies to Build Resiliency and Competitiveness"

Good morning. Chairman Sullivan, Ranking Member Markey, and Members of the Subcommittee, thank you for providing me the opportunity to testify today regarding the United States' economic relationship with the People's Republic of China (PRC). We are at historic cross-roads in the U.S.-China relationship, as the steps we take now will chart the course for U.S. economic and technological leadership, and will shape the landscape for the democratic world for decades, and possibly centuries to come.

The Department of Commerce's International Trade Administration is responsible for strengthening the competitiveness of U.S. industry in the United States and global marketplace, increasing investments in America, monitoring compliance with U.S. trade agreements, and enforcing U.S. trade laws. At Industry and Analysis (I&A), we are, in particular, responsible for working with businesses to develop international trade and investment strategies for a range of industries from the manufacturing sector to the financial services sector, including industries that are critical to the United States' national security interests. I&A also leads the Commerce Department's participation in the Committee on Foreign Investment in the United States (CFIUS), a committee that reviews certain specific foreign investments and real estate transactions in the United States for their impact on U.S. national security.

Today, I would like to speak about challenges to the United States' national security industries and set the stage for the successful commercial growth of our most critical sectors. In 2017, the U.S. Government began, for the first time, to confront head-on the challenges posed by China's predatory practices. Those challenges had been ignored for decades and, as a result, over the course of the past 40-plus years, the United States has continuously lost capabilities in sector after sector in manufacturing, technology, and services that are essential to our national security. In goods alone, the offshoring of manufacturing has created supply chain vulnerabilities across hundreds of critical products, ranging from semiconductor and electronics manufacturing to the development of active pharmaceutical ingredients. This has led to job losses of between 3.4 to 3.7 million between 2001 to 2018.[1] In key sectors such as communications equipment, electronics and computer technology, we ceded up to 40 percent of

[1] Scott, Robert; Mokhiber, Zane, Economic Policy Institute, "*Growing China Trade Deficit Cost 3.7 Million American Jobs Between 2001 and 2018*," (Jan. 30, 2020) https://www.epi.org/publication/growing-china-trade-deficits-costs-us-jobs/; *also* Census Data and Department of Commerce calculations.

the domestic market share to Chinese imports, and globally China has captured 40 percent of market share in those sectors as well.

To underscore with examples of where that leaves us, the United States does not have the domestic supply chains required to manufacture many key electronic components for our telecommunications systems, or many active pharmaceutical ingredients for medicines to serve America's health needs. Nor does the United States process the rare earth elements that produce magnets that are essential for military and weapons uses, as processing is now dominated by China. Even the more mature steel and aluminum industries have been experiencing existential challenges, as global overcapacity continues to weaken American firms. Where the United States was once the undisputed leader in technological innovation and industrial advancements across the board, it is now struggling to remain competitive in many key industries.

There are two classes of state actors in the global economy. The first class is comprised of nations that generally adhere to their obligations under the rules and principles of the global economic and trading system, as enshrined in international organizations such as the United Nations, International Monetary Fund, Organization for Economic Cooperation and Development, and the World Trade Organization (WTO). The second class is comprised of nations that either do not adhere (or selectively adhere) to these rules and norms, or actively circumvent them. While both classes of nations can introduce distortions into the global economic order – for example, through corporate subsidies and discriminatory nontariff barriers – the distortions can be managed when dealing with rules-based state actors and market-oriented economies. Here, international agreements may provide viable legal mechanisms to address non-competitive, market-distorting behavior, and states have historically adhered to their binding commitments or improved their practices when compliance fell short.

The Chinese Communist Party (CCP), on the other hand, does not just fall within this second class of state actors. It is also, by far, the most distortive economic actor that the global trading system has ever encountered. Not only are the current rules of international trade and monetary policy largely ineffective when dealing with China but, as a non-market economy under the tight control of the CCP, the government of the People's Republic of China flagrantly flouts those rules when it believes it is in its interest to do so, and shows no intention of reforming to a market-based system or adhering to its international obligations when those rules frustrate its national industrial goals. And because of China's size and scale, it has been able to weaken international supply chains and disrupt the global economy significantly. In this respect, the threat from China is formidable, and it is the largest threat the United States has encountered to date.

But we need to remember that this threat is nothing new, it has its roots in the Cold War. Khrushchev famously said "We," meaning the Sino-Soviet bloc, "declare war upon you," the United States, "in the peaceful world of trade. We will declare a war; we will win over the United States." Again, quoting from the Prime Minister of the Soviet Union, "We," again referring to the Communist states, "value trade less for economic reasons and most for political reasons." The hearing transcript for the Trade Act of 1962 includes these powerful statements. Perhaps in response to this threat, in the "Statement and Purpose" subsection of the Trade Act of 1962, 19 U.S.C. 1801, Congress explicitly enacted into law the goal of Chapter 19; it is *inter*

alia, "through trade agreements affording mutual trade benefits" to "prevent Communist economic penetration." This provision is still valid today precisely because the threats continue today. And after 1979, when the United States formally normalized trade relations with China, the PRC government accelerated its plan to augment global economic and military strength in a quest that it concedes will ultimately lead to a great power struggle against the United States.

The PRC government's weapon of choice is predatory economic tactics, and it has successfully used such tactics to disrupt global supply chains and weaken the technological advancements of the United States and its Western allies. China has transformed itself into the epicenter of global commerce, has centralized manufacturing and research and development (R&D) hubs within its own borders and, with this, it has accumulated the power to influence all economies that are dependent on it.

CHINA'S USE OF PREDATORY ECONOMIC TACTICS TO CAPTURE CRITICAL SUPPLY CHAINS AND TECHNOLOGY

In order to understand the PRC government's predatory economic strategy, it is important to understand the specific trade tools that it deploys. Indeed, China's most effective tools, by design, are those that are governed by weak or non-existent international rules and disciplines. To understand a "strategic competitor" or an "adversary," one has to understand their tactics. To counter those tactics, we need to consider how our laws need to be strengthened.

Case in point: China's economy has grown in large part because of the massive subsidies it provides to industries, and the lack of transparency on the subsidies it provides results from its failure to notify them completely to the WTO, as well as the absence of effective WTO rules governing the types of market-distorting industrial subsidies used in China.[2] It is difficult to legally challenge what we do not know about or what the rules do not cover. Moreover, China leverages its self-designated developing country status to avoid complying with existing WTO rules and obligations, and WTO rules are generally silent on how a member state can challenge another country's self-designated status.

Next, the PRC government takes advantage of the absence of applicable international rules over state-owned enterprises (SOEs) to funnel massive amounts of capital and other resources to SOEs with the well-publicized intent of dominating strategic sectors worldwide. The PRC government also distorts prices and costs throughout its economy (e.g., land and property, energy, wages, and raw materials) through direct price controls and to export undervalued goods and services worldwide, thereby weakening the competitive positions of

[2] Examples include Chinese government subsidies that constitute unlimited guarantees to corporations, subsidies to insolvent or ailing enterprises lacking credible restructuring plans (also known as "zombie" companies), subsidies that encourage global overcapacity, subsidies to firms unable to obtain long-term financing from independent commercial sources that are operating in sectors or industries in overcapacity, and direct debt forgiveness.

market-based firms. Dangling possible access to China's large consumer market and making available cheap labor, goods and services are also how China lures foreign manufacturing capacity and technological know-how into its own borders. And as the CCP controls the government of a sovereign state, it knows full well that its non-market economic system is unaffected by legal challenges or the prospect thereof by the rest of the world; even possible losses of legal challenges at the WTO may not be incentive enough to compel China to reform a system that has served it so well and eroded the competitive positions of its adversaries so quickly.

Just as alarming, the PRC government takes advantage of the dearth of rules governing global overcapacity to flood world markets with distortedly low-priced goods. In 2019, China's overcapacity significantly depressed global prices in the fiber optical cable market. Its strategy is to eliminate competitors and obtain absolute control over this critical 5G infrastructure asset. The PRC government has previously deployed the same strategy in the steel and aluminum sectors, among many others, and the same strategy will create excess capacity in new sectors in the future. And notwithstanding the fact that the 2020 coronavirus pandemic has dramatically reduced demand for steel and aluminum products worldwide, China has once again ramped up steel and aluminum production and dramatically increased inventories, contributing to drastic global price depression. This illustrates the national security threat to our steel and aluminum industries and why the President imposed Section 232 tariffs to address the impact of overcapacity and the threat posed by steel and aluminum imports. Outside the United States, however, the global surge continues and China's actions are still destabilizing the global steel and aluminum industries.

The PRC government is further exploiting opportunities abroad to monopolize strategic ports and mines (among other assets). State-backed Chinese investors own 10 percent or more of equity in ports in Europe, and it has major deals in Greece, Italy, Spain, France, the Netherlands, and Belgium. This is in addition to a growing number of investments in more than 40 ports in North America, South America, Eastern Europe, the Middle East, Africa, Central Asia, South and Southeast Asia, Australia, and the Pacific. The PRC government is similarly increasing control of the raw materials necessary for manufacturing high-technology products (*e.g.*, phones, vehicles, advanced energy storage systems, and magnets) that are sourced from a small number of countries, and for which substitutes are unavailable. Operating in niche markets with limited transparency, often in politically unstable countries, Chinese firms continue to capture supplies of cobalt, graphite, lithium, nickel, niobium, and platinum, to name just a few. Because these minerals and metals are finite assets that cannot be replaced, China is able to exert influence over the rest of the world by withholding access to these assets to compel nations to bend to its will.

Additionally, in its never-ending quest for technological superiority and control over key positions in the industrial value chain, the PRC government regularly has supported or directed the theft and misappropriation of U.S. technology and intellectual property (IP). Monetary damages accrued to the United States are estimated to range from $50 billion to as high as $600 billion annually. Moreover, by making short-lived market access promises to cutting-edge technology companies, the PRC government pressures the most technologically-advanced firms to transfer IP and sensitive data to it. The PRC government ultimately uses the IP it extracts from companies to displace them from the market. China's increased dominance in key

segments of the industrial value chain further cements its technology transfer approach. Even where Chinese firms are perceived to "collaborate" in technology development, take for example Huawei's announcement that it plans to build a $1.2 billion optical fiber research facility in the United Kingdom, the gains are only one sided.[3] Chinese companies will, as directed by the PRC government, benefit from scientific research and collaboration with international scientists abroad, resulting in some cases in the repatriation of technology to generate overcapacity to eliminate competition and obtain a monopoly position. In sectors like 5G, where optical fiber cables provide the infrastructure for an impending technology revolution, the national security implications are obvious.

It is also reported that the Chinese government, this year, is implementing a nationwide credit rating system for all corporations – foreign-owned or Chinese-owned – operating within China. Companies handling sensitive personal data and proprietary technical information will be required to transfer that data to the Chinese government. The European Chamber reports this credit rating system as amounting to "life or death" for companies. [4]

China's engagement in international standards as a way to influence the global technology market also is of great concern, but it is often not fully understood. To illustrate this attempted influence, take for instance the fact that, from 2011 to 2019, the number of Chinese-led technical committees in the International Organization for Standardization, one of the largest international standards setting organizations, increased by 75 percent.[5] Further, China has strategically increased its participation in the International Telecommunication Union (ITU), an agency of the United Nations responsible for coordinating telecommunications operations and services, with the hopes of expanding its influence around the globe. In fact, in key technology working groups of the ITU, China alone comprises 40 percent of participants.[6] Moreover, China's press into international standardization ranges from introducing weak proposals into the standards development process, flooding the organizations with low-quality proposals that detract from and take resources away from sound proposals, to making financial contributions as a way to wield power over those organizations and to punish member companies and countries

---

[3] Gold, Hadas, CNN, "*Huawei to Build $1.2 Billion Cambridge Facility as It Faces Uncertain UK Future*,"(June 25, 2020) https://www.cnn.com/2020/06/25/tech/huawei-cambridge-uk/index.html.

[4] European Chamber of Commerce, "*European Chamber Report on China's Corporate Social Credit System, A Wake Up Call for European Businesses in China*," (Aug. 28, 2019), https://www.europeanchamber.com.cn/en/press-releases/3045/european_chamber_report_on_china_s_corporate_social_credit_system_a_wake_up_call_for_european_business_in_china.

[5] Kamensky, Jack, China Business Review, "*China's Participation in International Standards Setting: Benefits and Concerns for U.S. Industry*," (Feb. 7, 2020) https://www.chinabusinessreview.com/chinas-participation-in-international-standards-setting-benefits-and-concerns-for-us-industry/.

[6] Department of Commerce calculations.

that do not side with its agenda. Indeed, China's participation in international organizations has become a vehicle to advance its One Belt One Road Initiative, and the more influence China has over standards development, the more likely this initiative will succeed.

Additionally, China uses other international organizations to advance its global ambition, including the Belt and Road Initiative. To illustrate, it has been reported that the head of the UN Department of Economic and Social Affairs used his position to discriminate against people and organizations who were drawing attention to the CCP's repression of the Uighur ethnic group. The World Health Organization's capture by the Chinese government, by failing to alert countries to the rapid transmission of the coronavirus, is yet another recent example. Even more to the point, if the Chinese government is currently threatening to retaliate against Nokia and Ericsson for the EU's possible move to ban Huawei from their 5G systems,[7] imagine the types of influence that China could wield if it is able to dominate global standards organizations and the standards themselves.

Finally, it is worth emphasizing that because China is a sovereign state, foreign laws can never be sufficient to fully address its conduct. In fact, the PRC government takes advantage of the United States' lack of an extradition treaty with it to advance cyberattacks on sensitive U.S. assets. The attacks not only obtain proprietary trade secrets from companies and sensitive personal information about American citizens from servers, but these attacks also target crucial weapons systems and sensitive military technology (well-documented examples include attacks that extracted sensitive information about U.S. submarines, cryptographic systems, the F-35 Joint Strike Fighter, and anti-ship missiles that are crucial for deterrence and developing countermeasures). China's medium of cybertheft also includes stealing computer software source codes, design technology, and technical product specifications. And the PRC government continues to violate its 2015 bilateral commitment to the United States in which it had vowed to refrain from stealing and misappropriating U.S. IP.

The tactics used by the PRC government over the course of the past 40 plus years have enabled the country to move its economy from the 12th largest in the world ($191 billion gross domestic product, GDP (current prices), in 1980) to the second largest ($14 trillion GDP (current prices) in 2019); become the second largest foreign holder of U.S. debt at $1.09 trillion in 2019 (the first largest being Japan holding $1.27 trillion), and grow as the world's largest exporter of goods. Indeed, the United States' largest bilateral trade deficit is with China ($345.6 billion in deficit in goods in 2019). In addition, China today holds uniquely powerful positions in the most critical supply chains in the world including rare earths elements, medical equipment and supplies, pharmaceuticals, and electronics.

The past policies of the United States did not effectively impede or curtail China's rise as a predatory economic actor. To build our seemingly efficient supply chains, we flocked to China

[7] Lin, Liza; Woo, Stu; Wei, Lingling, "*China May Retaliate Against Nokia and Ericsson If EU Countries Move to Ban Huawei*," Wall Street Journal (July 20, 2020), https://www.wsj.com/articles/china-may-retaliate-against-nokia-and-ericsson-if-eu-countries-move-to-ban-huawei-11595250557.

as the low-cost producer of virtually every link in the chain, allowed the PRC government to build reserves of U.S. dollars which it used to devalue its currency, traded our most sensitive intellectual property in exchange for short-term market access and profits, and did not adequately use legal enforcement tools to protect our industries. Our motives were short-sighted, and we failed to sufficiently anticipate the vulnerabilities that this trading relationship would create.

As a result, we willingly transferred our debt and exported our manufacturing capabilities (and jobs) to a non-market economy where market principles, transparency, and predictability do not exist. By doing this, we created a global economy where distorted prices and non-market conditions are allowed to proliferate. We also put China in control of our revenue stream. This vulnerability is often not discussed among policymakers, but it is important to emphasize: within our highest-technology sectors, substantial revenue comes from U.S. exports to China. This means that China, by controlling America's revenue stream, also controls America's ability to earn income and fund R&D. This is an extraordinary vulnerability that, if unaddressed, will be used by the PRC government to further halt America's technological progress.

RESHORING CRITICAL SUPPLY CHAINS

Traditionally, economists have viewed calls for countries to pursue policies aimed at protecting national security production capacity skeptically. They argued that a nation could, in a globalized world, always turn to other countries if the domestic supply chains eroded at home. However, what we have learned from the coronavirus crisis is that borders do matter because any state has the sovereign right, and ability to, restrict exports to the rest of the world. Indeed, the PRC government strategically withholds exports: (1) as a bargaining chip to extract concessions from trading partners; or (2) to punish trading partners that do not bend to its will. Even our allies introduced earlier this year – at the height of the pandemic – emergency export restrictions over much needed medical equipment in order to provide for their own citizens to the detriment of neighbors in need.

These facts should serve as an important reminder to the United States that the security of domestic supply chains is essential, and it must be regained because the basic political and economic unit should *always* remain the nation-state. Indeed, the protection of American citizens requires that the United States' vulnerable supply chains be strengthened, and a major component of supply chain resiliency must be reshoring. But how can the United States reverse the excessive offshoring that has occurred over the course of the past 40 years?

The problem is complex, but it can be solved through a whole-of-Government approach. That is, if we collectively are prepared to tackle difficult policy questions, even those that may run counter to long-held economic biases. To the extent that those biases once formed policies that incentivized critical industries to offshore, then logically they need to be revised or reversed.

Understanding what has led to the degradation of our supply chains, then it stands to reason that a comprehensive reshoring strategy must remedy those causes. At the outset, the United States must systematically and routinely identify all products, goods, and technologies that are critical to national security to address the country's dependency on imports from strategic competitors, whether in a time of war, cyber-attack, pandemic or other national

emergency. This Administration – my office in particular on behalf of the White House – has begun doing this. We need to continue this on a permanent basis. An additional component here is measuring the flow of technology if it is now as equally as important, and in many instances more important, than the traditional "national security good."

A second essential component of a reshoring strategy is incentivizing inward investments in domestic manufacturing and R&D activities. We have begun doing this to boost innovation and economic growth through tax cuts. A whole-of-Government approach, in partnership with Congress, will continue to make this effort successful.

Third, we have in our arsenal of tools powerful U.S. Government procurement authority, including the Defense Production Act authority, to provide capital to new American investments and also as a tool to generate demand, through U.S. Government purchases, for national security-related items that are produced within the United States. Reliance on Government procurement authority is what will compel many companies to take a leap of faith and re-invest in the United States. This is an important tool that we are using and should be empowered to use even more.

Fourth, it is, of course, axiomatic that U.S. investments must be encouraged to grow to commercial scale in order to compete against more mature foreign competitors. Further, an industry's commercial viability will generate robust upstream and downstream supply chains, draw in new market entrants to enhance production efficiency and moderate prices, attract greater private sector investments, and encourage competition to accelerate R&D. These are the fundamental building blocks of a resilient domestic supply chain.

Finally, we have the ability to increase exports of all U.S. firms – including those that re-shore to the United States – through trade agreements. We have begun to increase exports thorough the U.S.-Mexico-Canada Trade Agreement and the U.S.-Japan Trade Agreement, and we should continue to encourage greater exports through new trade deals.

With the support of Congress, we can build the strongest supply chain in the world, enhance our comparative advantage with allies, and create an ecosystem where market-based principles prevail and market distortions are eliminated. We have begun doing this; we can do more together, which is why this hearing is so important.

CONCLUSION

Historically, through times of adversity, the United States has led the world out of war and economic turbulence into recovery. And now too, the world will look to the United States to lead the way in solving today's supply chain challenges. It should not be forgotten that the global economy of the 20th century was developed by the United States and, although China is aggressively seeking to shape the global economic order of the 21st century, it is not too late to act. While the United States remains the largest economic power in the world (a status that is not guaranteed as China's exponential growth continues), it has the ability and leverage to act in coordination with allies. Time is of the essence, and our supply chain vulnerabilities are too great to await another national security crisis that may expose this country to even more devastation and destruction.