DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

"COUNTERING CHINA: ADVANCING U.S. NATIONAL SECURITY, ECONOMIC SECURITY, AND FOREIGN POLICY"

HEARING BEFORE:
THE SENATE COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

Elizabeth Rosenberg,
Assistant Secretary for Terrorist Financing and Financial Crimes
U.S. Department of the Treasury

May 31, 2023

WRITTEN TESTIMONY

Chairman Brown, Ranking Member Scott, and Distinguished Members of the Committee:

Thank you for the opportunity to testify today on "Countering China: Advancing U.S. National Security, Economic Security, and Foreign Policy." I also want to thank the Committee for its work on addressing our relationship with the People's Republic of China (PRC). Your partnership is critical to clearly convey to the leaders of the PRC that the United States speaks with one voice in advocating for our national interests and protecting our national security.

The United States and the PRC are the two largest economies in the world. For decades, the PRC's economy grew as it implemented market reforms and opened itself up to the global economy. And despite the current tension in our relationship, cooperation between our two countries is absolutely critical in addressing important global challenges like the climate and managing international debt distress. As Secretary Yellen has recently noted, the United States does not seek conflict, but rather a constructive and fair economic relationship with China, one where we can work together, when possible, for the benefit of our countries and the world.

That is why we seek expanded engagement with the PRC to work through the difficult issues that we face. While no two countries' interests will ever perfectly align, responsible nations must ensure that those differences do not threaten each other's safety and security.

Our economic approach to China is guided by three objectives: securing the national security interests of the United States and our allies and partners and promoting respect for human rights; seeking an economic relationship with China that fosters growth and innovation in both countries through healthy competition; and cooperating on the urgent global challenges of our day.

As a steward of the U.S. economic and financial system, the Department of the Treasury plays a vital role in protecting U.S. national security. For most of the post-9/11 era, Treasury's targeted national security work involved cutting terrorists and WMD proliferators off from the U.S. and international financial system. But now, in addition to addressing these threats, Treasury plays a key role in conducting broader economic statecraft to advance a host of our national interests.

As I have responsibility for coordinating Treasury policies to address, expose, and target national security threats, I will address security challenges related to the PRC, and the tools at Treasury's disposal to address them.

<u>Security Challenges Related to the PRC</u>

As an overarching principle, we deploy economic tools in line with the principles that Secretary Yellen has laid out: narrowly scoped and targeted to clear objectives; easily understood and enforceable, and readily adaptable when circumstances change; and whenever possible, coordinated with our allies and partners.

The first of our national security concerns related to the PRC is its challenge to global norms—norms that have maintained peace and had a part in enabling the PRC's economic growth.

Just recently at the G7 Hiroshima Summit, leaders discussed economic coercion. As the G7 leaders recognized, economic coercion "not only undermines the functioning of and trust in the multilateral trading system, but also infringes upon the international order centered on respect for sovereignty and the rule of law, and ultimately undermines global security and stability." Specifically, we have seen instances when the PRC has not only targeted U.S. persons, but also those located in our allies and partners like Australia, Canada, South Korea, the Philippines, and Lithuania. Another way we have observed China exploit economic vulnerabilities and dependencies is through enabling corruption. Take, for example, Wan Kuok Koi, a PRC national and former member of the Communist Party of China's Chinese People's Political Consultative Conference. Wan, also known as Broken Tooth, and his organization, the World Hongmen History and Culture Association, were designated by Treasury in December 2020 for corrupt practices, specifically the use of economic and business influence to co-opt elite figures in Malaysia and Cambodia. It should come as no surprise to Beijing that the economic, finance, and trade teams among the G7 are actively thinking through ways to build resiliency and support one another as well as other nations.

We also see efforts by PRC-related actors to conduct economic espionage against sensitive sectors of the economy. A recent example is the 2022 criminal prosecution by the Department of Justice and sentencing of Yanjun Xu, a PRC intelligence officer ultimately convicted of attempting to steal technology and proprietary information from aerospace companies based in the United States and abroad. This opacity in the PRC military-industrial complex and its military-civil fusion strategy is a national security concern of the United States and one of the reasons why many PRC aerospace companies are currently subject to economic restrictions, including from the U.S. Treasury.

We are also concerned about PRC-based transnational crime, including professional money laundering, cyber-criminal networks, and drug trafficking. Last year, Treasury submitted to Congress our assessment on money laundering threats emanating from the PRC, which highlighted many of these criminal activities. We continue to pay close attention to this type of criminal activity, and on April 23, Treasury identified and sanctioned Wuhan Shuokang Biological Technology Company and its leadership for the sale of fentanyl precursor chemicals. This action complemented indictments from the Department of Justice last month that connected these PRC companies to drug cartels in Mexico. These actions not only are against the letter of U.S. law and contrary to our national security interests—they also have had a devastating effect on our communities.

Nor can we overlook PRC's human rights abuses. Treasury has acted to promote accountability for the ongoing abuses in Xinjiang, Tibet, and Hong Kong. In addition, we have acted to promote accountability for PRC-based entities connected to serious human rights abuses, such as the Treasury designations of Dalian Ocean Fishing, Pingtan Marine Enterprise, and their affiliates. Over the years, vessels affiliated with Pingtan violated multiple countries' laws across the Pacific Ocean, including in Ecuador and Indonesia. Dalian Ocean withheld food and pay from their crew, refusing to let some of them disembark for over a year. On one vessel where crew were abused, five crewmembers died.

Another growing concern we have is the PRC's role in geopolitical conflict around the world. While the PRC seemed initially apprehensive about its economic relationship with Russia after Russia's full-scale invasion of Ukraine, we have seen bilateral China-Russia trade tick up, including certain transactions that the United States has now identified as circumventing U.S. sanctions and export control laws. Take King-Pai Technology Hong Kong, for example. This PRC-based supplier, now subject to blocking sanctions as well as export restrictions on the Commerce Department's Entity List, supplied the Russian military-industrial complex with components used in cruise missile guidance systems. Another example is designated PRC-based firm Spacety (Changsha Tianyi Space Science and Technology Research Institute Co. LTD), which sold radar satellite imagery that enabled the transnational criminal organization Wagner Group to enhance its combat operations in Ukraine on behalf of Russia. In coordination with our interagency partners, we will continue to expose and disrupt PRC entities that provide support for the Russian war effort.

The PRC has also been troublingly consistent in its support for North Korea, which allows Pyongyang to conduct numerous weapons tests contrary to international law. In the meantime, North Korea has relentlessly worked to maintain and improve its weapons systems, including an ICBM capable of striking the continental United States, and multiple missiles it has flown over inhabited Japanese territory. These increasing capabilities, combined with the hostile rhetoric coming from North Korea, are direct threats to the national security of the United States and its partners and require a U.S. response; and we believe the PRC can and should play a more constructive role in stabilizing the region.

Finally, we are closely watching the PRC's own rapid militarization of international spaces. This militarization takes many forms. Earlier this year in the South China Sea, for example, the PRC Coast Guard directed a military-grade laser at Philippine Coast Guard personnel and just last month, the PRC Coast Guard also aggressively maneuvered near Philippine patrol boat lawfully operating within the Philippines' Exclusive Economic Zone (EEZ), nearly causing a collision. As Department of Defense officials at multiple levels have attested, the PRC has also increased activity along its border with India, and routinely engages in risky operational behavior in international airspace over the East and South China Seas. Each time the PRC conducts risky military activities, there is a chance for a mistake or miscalculation, which again goes directly against our national security interests in preserving freedoms of navigation and overflight and keeping our allies and partners secure. This is why the People's Liberation Army is already subject to many financial and economic restrictions—we do not want funds and goods to go to the PLA to enable this type of destabilizing behavior.

Treasury's National Security Tools

I want to turn now to our tools at Treasury, and how we deploy them in service of our national security concerns.

First, Treasury publicly exposes threatening activity. This can, for example, take the form of targeted financial sanctions, when we designate individuals and entities undermining U.S. national security. By publicly outing these individuals and entities through a designation,

financial institutions and other organizations are able to build a fuller picture of the illicit activity and take action to distance themselves from the threats.

The second way we act to protect U.S. national security interests is through targeted disruption and interdiction efforts. Treasury regularly engages the private sector directly, providing information to help financial institutions, money service businesses, and other actors in the economic and finance space to identify and disrupt violations of our sanctions laws and regulations. Treasury also engages partners and allies who share similar concerns and are willing to take joint actions and enforcement.

A third way we protect our national security interest is by raising international financial standards and building partner consensus. Leadership in the Financial Action Task Force, the international standard-setting body for anti-money laundering and countering the financing of terrorism, is a major way we accomplish this. For example, my team helps lead the international virtual assets contact group, working to define the rules of the road for international financial systems in regulation of digital assets and countering their use in money laundering. By leveraging this international forum and building consensus around model laws and best practices, we increase the costs for actors to reject these norms.

To conclude, the United States can effectively manage our relationship with China by clearly conveying our interests and intentions, and by talking to each other about real examples, as I have done today. Indeed, the health of the global economy rests on how we, both the United States and the People's Republic of China, can manage our relationship and address pressing shared challenges. And while it is my job to address our national security interests through financial measures, I share Secretary Yellen's view: the world is big enough for the both of us. Our path is not preordained nor are we destined for open conflict, so long as we both choose to communicate clearly and act responsibly.

UNITED STATES DEPARTMENT OF COMMERCE
Assistant Secretary for Export Enforcement
Washington, D.C. 20230

Statement of
Matthew S. Axelrod
Assistant Secretary of Commerce for
Export Enforcement
Before the Senate Banking, Housing, and Urban Affairs Committee
Hearing Entitled, "Countering China: Advancing U.S. National Security, Economic Security, and Foreign Policy"

May 31, 2023

Chairman Brown, Ranking Member Scott, distinguished Members of the Committee, thank you for inviting me to testify on the Commerce Department's ongoing efforts to enforce U.S. export controls and to help deny the People's Republic of China (PRC) unauthorized access to U.S. technologies.

I currently serve within the Commerce Department's Bureau of Industry and Security as the Assistant Secretary for Export Enforcement. By passing the Export Control Reform Act of 2018 (ECRA), Congress provided Export Enforcement, the side of Bureau of Industry and Security that I oversee, with robust administrative and criminal enforcement authorities. My team of law enforcement agents and analysts use those authorities to conduct a mission essential to America's national security: keeping our country's most sensitive technologies out of the world's most dangerous hands.

At no point in history has this mission been more important, and at no point have export controls been more central to our national security, than right now. Our current geopolitical challenges, the increasingly rapid development of technology with the potential to provide asymmetric military advantage, and the countless ways in which the world is now interconnected, have raised the prominence and impact of export controls in unprecedented ways.

Each year, the Office of the Director of National Intelligence publishes the Intelligence Community's Annual Threat Assessment, which details the Intelligence Community's (IC's) view of the gravest national security threats faced by the United States. The differences between the first such assessment, issued in 2006, and this year's assessment are striking. In 2006, the DNI stated on the assessment's very first page that "terrorism is the preeminent threat to our citizens, Homeland, interests, and friends." The 2006 assessment's first section is on the "Global Jihadist Threat," followed by a section on "Extremism and Challenges to Effective Governance and Legitimacy in Iraq and Afghanistan." Analysis of the threat posed by China does not appear until page 20.

Compare that to this year's assessment and you will see how significantly our national security landscape has changed since 2006. The first four sections of this year's assessment each focus on a different nation-state actor, with China first, followed by Russia, Iran, and North Korea. As the assessment notes on its first page, "[w]hile Russia is challenging the United States and some norms in the international order in its war of territorial aggression, China has the capability to directly attempt to alter the rules-based global order in every realm and across multiple regions, as a near-peer

competitor that is increasingly pushing to change global norms and potentially threatening its neighbors."
The assessment later goes on to point out that "China will continue pursuing its goal of building a world-class military that will enable it to try to secure what it views as its sovereign territory, attempt to establish its preeminence in regional affairs, and project power globally while offsetting perceived U.S. military superiority," "is reorienting its nuclear posture for strategic rivalry with the United States because its leaders have concluded that their current capabilities are insufficient," and that China's "space activities are designed to advance its global standing and strengthen its attempts to erode U.S. influence across military, technological, economic, and diplomatic spheres."

Given this threat environment, the job of our Export Enforcement agents and analysts –preventing sensitive U.S. technologies and goods from being used for malign purposes by the Chinese government and other nation state actors – is more critical than at any other time in the organization's history. It's among the reasons why I'm so honored to lead such an expert and dedicated law enforcement team at this particular point in time. The team and I work every day to meet this unprecedented moment. More specifically, under my leadership, we have: (1) enhanced our enforcement policies; (2) expanded our partnerships at home and abroad; and (3) aggressively enforced our controls in a way that imposes real costs on those who seek to violate and undermine U.S. national security – both in China and elsewhere.

Enforcement Policy Enhancements

First, we have updated a number of our enforcement policies to ensure that our finite resources are best positioned to have maximum national security impact. A few highlights:

- On June 2, 2022, we published a regulatory change making our administrative charging letters public when filed (as opposed to the prior practice of making them public only after resolution), in order to provide the exporting community more timely insight into actions that we believe violate our rules. Just one month later, we published a charging letter against Far East Cable Co. Ltd., China's largest wire and cable manufacturer, based on allegations that it served as an illicit export channel for Zhongxing Telecommunications Equipment Corporation (ZTE) and delivered U.S.-origin equipment to Iran as part of an effort to conceal and obfuscate ZTE's Iranian business from U.S. investigators.

- On June 30, 2022, I announced policy changes to strengthen our administrative enforcement program. The changes included raising penalties when appropriate for more serious violations, prioritizing enforcement focus on the most serious violations while using non-monetary resolutions for less serious violations, eliminating "No Admit, No Deny" settlements, and dual-track processing of voluntary self-disclosures. As a result of these policy changes, our recent $300 million resolution with Seagate Technology, LLC ("Seagate") included an admission by Seagate to the factual conduct alleged in our Charging Letter – that Seagate continued selling millions of hard disk drives to entity-listed Huawei even after its only two competitors had stopped sales because of our Foreign Direct Product Rule (the Huawei FDPR). The Huawei FDPR imposes export controls on foreign items produced overseas from certain U.S. software and technology, including equipment, when destined for Huawei.

- On October 7, 2022, in conjunction with the promulgation of rules imposing new controls on China's procurement of advanced semiconductor manufacturing tools, advanced chips and related items, we issued a rule clarifying that when a foreign government fails to schedule end-use checks (i.e., physical inspections of exports to ensure they are in compliance with our regulations) in a timely way, that failure can provide a basis for the addition of unchecked parties to the Entity List. I also issued a memorandum outlining a two-step policy to address persistent scheduling delays of our end-use checks. Under the policy, if BIS requests an end-use check from a foreign government, that government then has 60 days to enable BIS to conduct the check – otherwise we may place the unchecked party on the Unverified List. After that, if 60 more days pass without the check being successfully completed, we may place the unchecked company on the Entity List. Prior to this policy change, the Chinese government had not allowed us to conduct a check in over two years. The policy led directly to improved cooperation with our pending checks. In the seven months since the policy was announced, we have completed over 90 end-use checks in China.

- On April 18, 2023, I issued a memorandum clarifying our policy regarding voluntary self-disclosures (VSDs) and disclosures of potential misconduct by others. It's long been understood that when a company finds out about a significant potential violation, and self-reports it, they get concrete VSD credit in the form of a reduced penalty. The memorandum makes clear that the converse is also true: if a company knows of a significant potential violation and affirmatively decides not to divulge it, we will consider that lack of disclosure as an aggravating factor in penalty calculations if we later uncover the violation. Separately, the memo clarifies that when a party informs us about another party's violation and that information allows us to take enforcement action, we will consider it "extraordinary cooperation" and treat it as a mitigating factor if the notifying party engages in prohibited conduct in the future. This policy clarification is designed to lead to an increase in disclosures, which in turn should lead to additional enforcement actions involving Chinese (and other) violators.

Technology Protection Partnerships

Second, given the scope of the threat that we face in protecting U.S. technology from misappropriation by the Chinese government and other actors, we acutely understand the need to amplify our efforts through robust partnerships. Domestically, we have developed such partnerships with industry, academia (through our Academic Outreach Initiative), the IC, Treasury components like the Office of Foreign Assets Control and Financial Crimes Enforcement Network, and sister federal law enforcement agencies like the Federal Bureau of Investigation and Homeland Security Investigations. In the past year, we have put out multiple joint alerts and advisories with these partners designed to educate industry and financial institutions on how best to comply with our rules and detect violations of them. These partnerships allow us in many instances to prevent diversions before they occur, and in others to impose costs on violators.

We also work closely with international counterparts, bilaterally, multilaterally, and through our end-use check program. Last year, our Export Control Officers (ECOs), augmented by our domestic-based Sentinel teams that deploy to global locations not covered by ECOs, conducted over 1,100 end-

use checks in over 50 countries to prevent the transshipment and diversion of U.S. items in violation of our regulations.

And, thanks in part to additional funds from Congress in the first Ukraine supplemental appropriations law last year, we have worked to expand our footprint and partnerships abroad, including stationing an analyst in Canada and ECOs in Finland and Taiwan this summer, implementing a data sharing arrangement with the European Anti-Fraud Office (OLAF), and establishing export enforcement coordination mechanisms with our Five Eyes (U.S., Australia, Canada, New Zealand, and the United Kingdom) and G7 counterparts to prevent illicit reexports to China, as well as to Russia, Iran, and elsewhere.

We have also entered partnerships designed to deliver concrete enforcement actions. On February 16, 2023, we announced the formation of the Disruptive Technology Strike Force in partnership with the National Security Division of the Department of Justice. The Strike Force works to protect U.S. advanced technologies from being illicitly acquired and used by nation-state actors such as China, Russia, and Iran to support: (1) their military modernization efforts; and (2) their mass surveillance programs that enable human rights abuses. We have established operational Strike Force cells in fourteen locations across the country, supported by an interagency intelligence effort in Washington, D.C. Each operational cell consists of agents from our Office of Export Enforcement (OEE), FBI, and HSI, as well as an Assistant U.S. Attorney. The Strike Force cells use all-source information (open source, proprietary, and classified) to pursue investigations and take criminal and/or administrative enforcement action as appropriate.

Just two weeks ago, Assistant Attorney General Matt Olsen and I announced the first wave of Strike Force enforcement actions, including arrests, indictments, and a temporary denial order in five different cases across the country. Two cases – one out of Los Angeles and the other out of San Francisco – involve defendants who allegedly stole sensitive American technology and shipped it to restricted Chinese entities. In a third case, from Manhattan, the defendant allegedly used a sanctioned Chinese company as a front company to aid Iranian ballistic missile procurement. According to the indictment, the defendant conducted transactions with an Iranian company to obtain isostatic graphite, a material used in the production of weapons of mass destruction. These actions illustrate how the Strike Force cells are prioritizing investigative and prosecutorial resources to target illicit actors, impose costs on violators, and harden supply chains to protect our most advanced technologies from being acquired or used by nation-state actors such as China.

Enforcement Actions

Third, I want to highlight some of the recent enforcement actions we have taken related to China this calendar year, beyond the work of the Disruptive Technology Strike Force described above.

On April 20, we announced the largest standalone administrative penalty in BIS history – a $300 million penalty against Seagate Technology LLC of Fremont, California and Seagate Singapore International Headquarters Pte. Ltd. of Singapore for continuing to ship millions of hard disk drives to Huawei after BIS's imposition of the Huawei FDPR. It is also the first enforcement case and penalty brought under the Huawei FDPR since that rule was issued in August 2020. In addition to the monetary penalty, Seagate is subject to a suspended five-year denial order that allows BIS to cut off their export privileges if they violate key terms in the agreement.

As part of the resolution, Seagate admitted to having engaged in the conduct alleged in our Proposed Charging Letter. Back in 2019, BIS placed Huawei and certain of its non-U.S. affiliates were put on the Entity List for posing a risk to U.S. national security. In August 2020, due to continued national security and foreign policy concerns, BIS imposed the Huawei FDPR to better address the continuing threat to U.S. national security and U.S. foreign policy interests posed by Huawei and its non-U.S. affiliates. At that time, there were only three major companies producing hard disk drives including Seagate. When the Huawei FDPR went into effect, two out of the three companies promptly, and publicly, stated that they had ceased sales to Huawei and that they would not resume such sales unless or until they received authorization from BIS. Despite this public declaration from its competitors, the third company, Seagate, continued to sell and became Huawei's sole source provider for hard disk drives. Seagate continued selling hard disk drives to Huawei until September 2021, more than a year after their competitors pulled out, and more than a year after the Huawei FDPR was published. The $300 million penalty is more than double the amount of profits they made from these sales.

On February 27, 2023, we imposed a $2.77 million penalty on 3D Systems Corp. for exporting controlled aerospace technology (including technical specifications for military electronics as well as those used in the development, production, operation, or repair of spacecraft) and metal alloy powder to China without the required license and for exporting controlled technology to Germany without the required license. In addition to our penalty, 3D Systems entered into coordinated settlement agreements with the Department of State and the Department of Justice.

On January 17, 2023, Jonathan Yet Wing Soong pleaded guilty to violating export control laws in connection with a scheme to secretly funnel sensitive aeronautics software to Beihang University, a university in Beijing on the Entity List due to the University's involvement in PRC military rocket systems and unmanned air vehicle systems. Soong, an employee of a NASA contractor, admitted that he willingly exported and facilitated the sale and transfer of restricted software knowing that Beihang University was on the Entity List. On April 28, 2023, Soong was sentenced to 20 months in prison.

Also on January 17, 2023, we issued a 10-year denial order cutting off the export privileges of Ge Song Tao following his conviction for conspiracy to attempt to illegally export maritime combat rubber raiding craft and engines to China. The joint case with FBI, ATF, NCIS, and DOJ uncovered that Ge used his company, Shanghai Breeze, and contacts with a U.S. Naval Anti-Submarine Warfare Officer to attempt to illegally export the items to the People's Liberation Army (PLA) Navy. The combat rubber raiding craft, which the Chinese military planned to reverse engineer and mass produce, was equipped with engines used by U.S. special forces and can be launched from a submarine or dropped by an aircraft. The items did not get to China.

On January 11, 2023, Broad Tech Systems, Inc., a California-based electronics distribution company, and Tao Jiang, its president and owner pleaded guilty to charges of conspiracy and ECRA violations. Jiang participated in a conspiracy to conceal information from BIS agents and U.S. Customs and Border Protection officers as part of a scheme to illegally export chemicals used in semiconductor manufacturing to an Entity Listed company in China. The Chinese company develops

electronics for early warning systems, air defense systems, airborne fire control systems, manned space systems, and other national large-scale projects for the PLA.

We also use the Entity List to restrict the ability of parties involved in activities contrary to U.S. national security or foreign policy interests to obtain U.S. exports. While the Entity List is a licensing tool, not an enforcement one, the overwhelming majority of Entity List nominations come from the BIS intelligence analysts I oversee and frequently have ties to investigations conducted by our law enforcement agents. Currently, there are nearly 700 Chinese parties on the Entity List, of which over 200 have been added since the beginning of this Administration.

As these cases and entity listings demonstrate, we leverage our administrative and criminal enforcement, as well as our regulatory authority, to address the diversion of advanced technologies – like semiconductors, marine engines, and satellite and rocket prototypes – that support China's military modernization efforts.

Conclusion

Thank you again for the opportunity to testify today on national security risks posed by the People's Republic of China (PRC) and what we on the Export Enforcement side of the Department of Commerce's Bureau of Industry Security are doing to combat them. As CIA Director William Burns has noted, China is the most important geopolitical threat that we face this century. And Export Enforcement's mission – keeping our country's most sensitive technologies out of the world's most dangerous hands – is a critical part of how the U.S. Government addresses the threat posed by the PRC.

As Beijing seeks to spread its technology-driven authoritarianism the world over, Export Enforcement remains hyper-focused on preventing the PRC from illegally obtaining sensitive U.S. items. By enhancing our administrative enforcement capabilities, multiplying our impact through work with partners, and aggressively pursuing both administrative and criminal enforcement actions to punish violators, we are committed to doing everything we can to meet this unprecedented challenge.

I thank the Committee for its support and look forward to your questions.

UNITED STATES DEPARTMENT OF COMMERCE
Deputy Assistant Secretary for Export Administration
Washington, D.C. 20230

Statement of
Thea D. Rozman Kendler
Assistant Secretary of Commerce for
Export Administration
Before the Senate Banking, Housing, and Urban Affairs Committee
Hearing Entitled, "Countering China: Advancing U.S. National Security, Economic Security, and Foreign Policy"

May 31, 2023

Chairman Brown, Ranking Member Scott, distinguished members of the Committee, thank you for inviting me to testify on behalf of the Commerce Department's, Bureau of Industry and Security (BIS) Export Administration's ongoing efforts to administer U.S. export controls and counter the People's Republic of China's (PRC's) military modernization, human rights abuses, and other activities contrary to our national security and foreign policy interests.

BIS is responsible for protecting U.S national security and foreign policy interests by ensuring that U.S. technology is not used by adversaries to harm the United States and by working to promote American technological leadership. This responsibility stems from our authorizing statute–the Export Control Reform Act of 2018 (ECRA)–which describes the policy goals for BIS's administration and enforcement of the export control system. While I am responsible for the regulatory side of the Bureau, my colleague, Assistant Secretary for Export Enforcement Matthew Axelrod, is charged with the enforcement side.

Through the Export Administration arm of BIS, we identify sensitive U.S. technologies that would give our adversaries an advantage, develop policies and strategies for protecting these technologies, and review license applications submitted by exporters to determine whether specific transactions are consistent with U.S. national security and foreign policy interests. We also analyze data, industry information and classified reporting to assess the effectiveness of our controls, the availability of foreign technology (including identifying sensitive technologies developed by ally and partner countries), and the foreign end users that require extra scrutiny before receiving U.S. technology.

Ensuring that U.S. and allied technology is not used against us is central to our approach with the PRC. In administering our export controls, we endeavor to take a multilateral approach. There are certainly times where unilateral export controls are necessary, however, as ECRA notes, "[e]xport controls that are multilateral are most effective[.]" Accordingly, foreign cooperation on our controls is a BIS priority. Moreover, as evidenced by our approach to Russia's further brutal invasion of Ukraine, multilateralism has reinvigorated our close and continuing international partnerships, particularly with countries in Europe and the Indo-Pacific.

As the G7 leaders reaffirmed on May 20, 2023, in the G7 Hiroshima Leaders' Communiqué,

> [E]xport controls are a fundamental policy tool to address the challenges posed by the diversion of technology critical to military applications as well as for other activities that threaten global, regional, and national security. We affirm the importance of cooperation on export controls on critical and emerging technologies such as microelectronics and cyber surveillance systems to address the misuse of such technologies by malicious actors and inappropriate transfers of such technologies through research activities.

National Security Advisor Jake Sullivan, channeling recent comments by European Commission President Ursula von der Leyen, observed in April that we are "de-risking and diversifying" with respect to the PRC on a narrow slice of technologies. We are not interested in decoupling. There are many areas in which the United States and the PRC can and should continue to cooperate. As we continue to stand up for our core national security and foreign policy interests, the world's two biggest economies should continue to engage in commercial trade that does not impact U.S. national security or foreign policy interests.

I. BIS's Perspective on the PRC National Security and Foreign Policy Threat

As Secretary Raimondo has stated: "China today poses a set of growing challenges to our national security. It is deploying its military in ways that undermine the security of our allies and partners and the free flow of global trade. . . ." The Chinese Communist Party (CCP) under President Xi Jinping has set a goal to develop the People's Liberation Army (PLA) into a "world class military" and overtake the United States and its allies by dominating certain advanced technology sectors such as artificial intelligence (AI), autonomous systems, advanced computing, semiconductors and microelectronics, quantum information sciences, biotechnology, and advanced materials and manufacturing.

To fulfill this vision, the PRC is going to great lengths to obtain key advanced technologies with military potential. It uses a military civil-fusion (MCF) strategy to deliberately blur lines between commercial sectors and military programs. This strategy is even more concerning where the PRC's government structure gives leadership the power to demand information and assistance from companies that have little choice but to agree. Accordingly, MCF, combined with the PRC's government system, has necessitated stronger export controls targeting predominantly commercial items that can be used in military applications.

In the face of this transformative challenge that is decidedly exacerbating threats to global peace and security, it is imperative that the United States and our allies safeguard our core technologies by continuously and proactively reviewing and updating our export control policies.

BIS has long restricted the PRC's access to advanced dual-use items, including technologies. Together with our interagency partners in the Defense Department's Defense Technology Security Administration, the Energy Department's National Nuclear Security Administration, and the State Department's Bureau of International Security and Nonproliferation, we appropriately leverage the tools in our toolbox to address this threat. This includes technology controls, identification of entities of concern, outreach and education initiatives, and international engagement.

We partner closely with the Departments of Defense, Energy, and State in a range of functions, including proposals to the multilateral export control regimes, amendments to the Export Administration Regulations (EAR), review of export license applications, and identifying specific end users of concern, because each of these agencies brings different, valuable considerations and understanding to the review of such applications.

To succeed in using our tools to contend with the strategic challenge posed by the PRC, our interagency and international partnerships are more valuable than ever before.
In today's testimony, I will discuss the long-standing controls we have in place for the PRC, technology controls adopted under the Biden-Harris Administration, the targeting of PRC entities of concern, and the measures we are taking to educate the public, as well as foreign partners, on the nature of and rationale for our controls.

II. PRC Dual-Use Export Controls and Licensing

BIS maintains comprehensive controls on the exports of sophisticated technologies to the PRC. BIS also controls low level technologies to preclude exports to untrusted end users, PRC military activities, and weapons of mass destruction (WMD) programs. This includes the imposition of license requirements for:

- all military and spacecraft items under BIS jurisdiction (which are subject to a statutory policy of denial);
- all multilaterally-controlled dual-use items;
- a large number of dual-use items with extensive commercial applications if the item is intended, entirely or in part, for a military end use or military end user in the PRC;
- all items under our jurisdiction if the item is exported knowing it will be used in certain WMD programs;
- all items under our jurisdiction if the item is exported knowing it is intended, entirely or in part, for military-intelligence end uses or end users in the PRC; and
- all items under our jurisdiction if the item is destined for a party on BIS's Entity List.

In addition, BIS prohibits certain U.S. person activities that would support WMD-related activities or military-intelligence end use or end users in the PRC, even if no items subject to our jurisdiction are involved, absent authorization. We are grateful to the Committee and others in Congress for enhancing our authorities in this regard as part of the Fiscal Year (FY) 2023 National Defense Authorization Act. We are actively working to implement these expanded authorities.

With our interagency partners, we review all of the license applications for the PRC to determine a risk of diversion to military end uses or end users, WMD end uses, or abuses of human rights. We evaluate license applications–taking into account open source and intelligence information–based on

the technology at issue, the country at issue, the entity using the item, other parties involved in the transaction, and how the item will be used. One of the primary factors we consider is the risk of diversion of the technology from the transaction details articulated in the license application instead to a country, end user, or end use of concern. We deny license applications where there is evidence of a substantial risk of diversion.

License applications submitted by exporters and reexporters to send items to the PRC receive close scrutiny by BIS and our interagency partners. In calendar year (CY) 2022, license applications for the PRC had an average processing time (APT) of approximately 90 days. This APT is significantly longer than the CY 2022 APT for non-PRC cases of 43 days. It is also longer than the CY 2021 APT for PRC cases of 76 days. As evidenced by this data, BIS with its interagency colleagues is taking the time to ensure that PRC licenses are carefully reviewed. We prioritize comprehensive review of relevant open source and intelligence information over speed.

In CY 2022, licenses reviewed for the PRC comprised approximately 13 percent of all applications reviewed by BIS. For items, including commodities, software, and technology (including domestic technology transfers, known as deemed exports), BIS and our interagency partners reviewed 5,064 export and reexport license applications. Of these, approximately 26 percent were denied or returned without action.

In general, statistics regarding the interagency licensing process must be considered in light of the inherent restraint exercised by U.S. companies that generally do not waste time or resources applying for licenses they know will be denied or subject to lengthy interagency review. U.S. exporters should, before filing license applications know the parties in their transactions, including intermediaries and the end user, as well as the end user's intended use of the item. Exporters who do not do this risk either a return of rejection or return without action of their license application. After reviewing BIS's extensive know-your-customer and red flags guidance, many U.S. exporters do not submit license applications for transactions they contemplate are likely to be rejected. In fact, applications for exports to the PRC dropped by 26.2 percent between CY 2021 and CY 2022 (although volumes are still higher than during the height of the pandemic).

III. Dual-Use Export Controls to Counter PRC Military Modernization

BIS's approach to the PRC is calibrated and targeted. Using a scalpel approach, we seek to restrict the PRC's military modernization efforts by restricting key, sensitive technologies without undercutting U.S. technology leadership and unduly interfering with commercial trade that doesn't undermine our national security and foreign policy.

We remain focused on aggressively and appropriately using our tools to contend with the long-term strategic competition with the PRC. Under Secretary Alan Estevez previously testified before this Committee, "We are closely reviewing our approach to China, seeking to maximize the effectiveness of our controls." To that end, we have prioritized a review of export controls related to quantum, the bioeconomy, and artificial intelligence.

An example of our approach is the October 2022 advanced computing and semiconductor manufacturing equipment rule, which restricted the PRC's access to critical artificial intelligence integrated circuits, supercomputing capability, and semiconductor manufacturing technology. The October 2021 controls on software for nucleic acid synthesizers, followed by this April's proposed rule on potential peptide synthesizer controls, further demonstrate this focus.

A. Proactively Restricting PRC Plans to Use U.S. Technologies Related to Artificial Intelligence and Advanced Semiconductors for Military or WMD Applications

The PRC's efforts to develop and employ advanced artificial intelligence (AI) in its military modernization, hoping to surpass the United States and its allies and our military capabilities, demanded a clear, strategic export controls response.

Artificial intelligence was described as "the quintessential 'dual-use' technology" in the 2021 Final Report of the National Security Commission on AI. The Commission noted that, "The ability of a machine to perceive, evaluate, and act more quickly and accurately than a human represents a competitive advantage in any field—civilian or military." AI capabilities—facilitated by supercomputing, built on advanced semiconductors—present U.S. national security concerns because they allow AI to be used to improve the speed and accuracy of military decision making, planning, and logistics. They can also be used for cognitive electronic warfare, radar, signals intelligence, and jamming. These capabilities can also create concerns when they are used to support facial recognition surveillance systems for human rights abuses. Advanced semiconductors are key to developing advanced weapon systems, exascale supercomputing capabilities, and AI capabilities.

Although the PRC has tried to characterize U.S. export control actions on advanced semiconductors, supercomputing, and AI as an economic measure aimed at restraining its economic growth, BIS focused solely on these clear national security and foreign policy considerations when issuing our rules.

We made several changes to U.S. dual-use export controls policy to the PRC to address our AI concerns:

- First, BIS implemented targeted restrictions on specific chips, and items containing such chips, that can be used in advanced computing and artificial intelligence applications. Through a new Foreign Direct Product (FDP) Rule, BIS further applied these controls to foreign-made chips that are produced with certain U.S. technology or tooling and PRC chip designs meeting the relevant parameters identified by our technical experts.

- Second, BIS implemented controls for chips and other items that will be used in or for supercomputers in the PRC or supercomputers destined for the PRC. Through another new FDP Rule, this control also applies to certain foreign-made items when destined for PRC supercomputers, including foreign-made semiconductors.

- Third, BIS expanded the scope of controls on 28 PRC entities previously on the Entity List that are involved in supercomputer-related activities or advanced integrated circuit-related activities. These parties are now subject to the Entity List FDP Rule that restricts the entities' ability to obtain foreign-produced chips and other items. BIS added additional PRC entities to the Entity List in December 2022, which are also subject to the Entity List FDP Rule.

- Fourth, BIS implemented new PRC-wide controls on exports of certain manufacturing tools essential for high-end chip production.

- Fifth, BIS imposed controls on the export of any item to a PRC semiconductor fabrication facility that is engaged in the development or production of advanced logic or memory chip

production. For these advanced fabrication facilities, we also imposed a license requirement on U.S. persons providing support to those entities.

- Finally, we imposed controls on items that will be used to develop or produce indigenous semiconductor manufacturing equipment in the PRC.

BIS's actions already are having an impact in the PRC. Since implementation of our controls, public reporting shows that the PRC is surging resources into its semiconductor sector. However, the PRC knows that money alone cannot solve its problem. Our cut-off threshold for advanced logic semiconductor manufacturing in the PRC is at 14 nanometers (nm). The PRC's sole semiconductor lithography equipment manufacturer, Shanghai Micro Electronics Equipment Group (SMEE), has not made any major advancements since achieving the generations-earlier 90nm equipment, in part due to the difficulties of obtaining components and servicing from abroad–difficulties increased by the December 2022 placement of SMEE on the Entity List by BIS. The PRC's largest semiconductor foundry, Semiconductor Manufacturing International Corp. (SMIC) has removed 14nm fabrication technology from the list of services on its website.

Although our measures have restricted the PRC's ability to indigenously produce advanced semiconductors, we know that the PRC is looking for ways to continue accessing these high-end chips. In this evolving technological landscape, we continue to review open source and classified information to address circumvention attempts, to track the impact of our controls, and to be proactive and nimble.

B. Countering PRC Use of Automated Peptides Synthesis to Develop Toxins

The Office of the Director of National Intelligence has assessed that advancements in dual-use technology, including synthetic biology and genomic editing, could enable the development of novel biological weapons that evade detection, attribution, and treatment. In particular, software for nucleic acid assembly and synthesis can be used to design and build functional genetic elements from digital sequence data. This data can then be manipulated to create novel pathogens or enhance existing ones.

For these reasons, in October 2021, based on a BIS proposal, we, along with our Australia Group partners—a multilateral regime consisting of 43 participating countries that focuses on the spread of chemical and biological weapons—imposed multilateral controls on software for nucleic acid assembly and synthesis. Additionally, in April of this year we sought public comment on the potential control of peptide synthesizers. These technologies make it quicker and easier to produce toxins and pathogens that can be exploited for biological weapons purposes. By adopting these controls, requiring a license to the PRC will help ensure that our biotechnology exports are not used for malign purposes.

IV. Controlling PRC End Users of National Security and Foreign Policy Concern

In addition to its technology-based controls, BIS increasingly has used entity-specific restrictions, primarily through the Entity List, to restrict trade to actors of concern in the PRC. Through the interagency End User Review Committee (ERC), BIS and our interagency partners review PRC companies, both state-owned and commercial, to determine if they are reliable recipients of U.S. technology.

Through the Entity List, we impose entity-specific license requirements on PRC parties based on specific and articulable facts that indicate that they have been, are, or are at significant risk of becoming involved in activities contrary to U.S. national security or foreign policy interests. We continually assess available open-source, proprietary, and classified information, in coordination with interagency partners, for imposing controls on additional PRC entities.

Generally, when a PRC party is added to the Entity List, anyone seeking to export, reexport, or transfer items under BIS jurisdiction to such a party must first obtain a license. BIS and our interagency partners in the Departments of Defense, Energy, and State review license applications for such PRC entities under the entity-specific license review policy published in the EAR, which is frequently a presumption of denial.

For entities not subject to a comprehensive presumption of denial, the Entity List provides clear policies on the types of items and transactions that may be approved on a case-by-case basis. Thus, companies are likely to only submit license applications for proposed export transactions qualifying for case-by-case review rather than those subject to a presumption of denial.

Currently, we have nearly 700 PRC parties on our Entity List – over 200 of those were added during the Biden-Harris Administration. They have been added for reasons including supporting PRC's military modernization and WMD programs, supporting Iran's WMD and military programs, facilitating human rights abuses in Xinjiang, and providing restricted items to Russia. These parties include those involved in AI, surveillance, biotechnology, microelectronics, and quantum computing.

For example, in December 2021, we added the PRC Academy of Military Medical Sciences and its eleven research institutes under the PLA's Academy of Military Sciences to the Entity List for using biotechnology processes to support PRC military end uses, including purported brain-control weaponry. In December 2022, we added Cambricon Technologies, one of the PRC's most valuable AI chip start-ups, and its subsidiaries for supporting PRC military modernization efforts. These entities are, or have close ties to, government organizations that support the PRC military and defense industry. Most recently, in March 2023, BGI subsidiaries BGI Research and BGI Tech Solutions were added for their collection and analysis of genetic data which contributes to the monitoring and surveillance of ethnic minorities in the PRC. In addition, in the Russia context, we have added companies in the PRC that attempted to circumvent regulations by aiding Russia's unconscionable invasion of Ukraine. Sinno Electronics, added June 2022, and others, were added to the Entity List for supporting Radioavtomatika, a Russian procurement firm for the Russian defense industry.

V. Engaging International Partners

Export controls can only be effective when other technology producers implement comparable controls. Consistent with ECRA, we know that export controls applied to items widely available from foreign sources generally are less effective. This is particularly true when we consider whether to apply export controls to an item that is manufactured both in the United States and the PRC. We also consider this factor when applying controls to technologies that are available in third countries. In such situations–to use a phrase that originates with former BIS Under Secretary Eric Hirschhorn–unilateral export controls are like damming half the river. BIS embraces the significant

responsibility to work with international partners to explain the rationale for our export control policies and, where possible, to include them in our efforts.

In light of these realities, we have reinvigorated our international partnerships over the last two years. In response to Russia's war on Ukraine, our dual-use export controls relationships with the 39 other governments that make up the Global Export Control Coalition are closer than ever.

Relatedly, working with the State Department and other partners, from FY 2021 to FY 2022, BIS more than doubled our capacity-building international engagement portfolio, from 23 to 61 engagements. We expanded our Export Control and Related Border Security (EXBS) activities from two and three countries in 2019 and 2020, respectively, to more than 21 countries in FY 2023.

Many of the controls we have imposed on the PRC involve a Foreign Direct Product rule. In these instances, we work closely with manufacturing countries to ensure that government and industry understand our controls and their application outside the United States. To maximize effectiveness of our controls, we have conducted government and industry outreach in Asia, Africa, Europe, and the Western Hemisphere. In each engagement, we endeavor to explain the clear national security rationale underpinning our controls.

VI. Conclusion

Dual-use export controls work has never been more relevant, or more effective. We are focused on aggressively and appropriate contending with the strategic technology threat posed by the PRC and will continue to appropriately and aggressively use the tools at our disposal to counter PRC efforts to outpace the United States and our allies to the benefit of the PLA.

Thank you. I welcome your questions.

Statement of Paul Rosen
Assistant Secretary for Investment Security
U.S. Department of the Treasury

Senate Banking, Housing, and Urban Affairs Committee Hearing

Good morning, Chairman Brown, Ranking Member Scott, and Members of the Committee. Thank you for the opportunity to speak with you today about this important national security issue.

At the Department of the Treasury, we understand the significant challenge China poses to the economic and national security interest of the United States. I manage the government's review of foreign investment into the United States for national security risks through the Committee on Foreign Investment in the United States (CFIUS). In this work we are focused on stopping the access and exploitation of sensitive technologies, infrastructure, data and other assets by those who have the intent and capability to harm our national security.

Recently, Secretary Yellen addressed the U.S.-China economic relationship. In her remarks, she conveyed that China and the United States can and need to find a way to live together and share in global prosperity. She also stressed the importance of our countries working together, when possible, for the benefit of us and the world.

At the same time, Secretary Yellen was crystal clear when it comes to national security: The United States will secure our national security interests and those of our allies and partners. We remain firm in our conviction to defend our values. We will not hesitate to defend our vital interests. And we will not compromise on national security concerns—even when they force trade-offs with our economic interests. She also made clear: we do not use our national security tools to gain competitive economic advantage or to stop China from growing. But we will fully and zealously exercise our economic tools to protect the national security of the United States, full stop.

CFIUS is one important tool to address national security that pursues these objectives. The Committee—comprised of the heads of several Executive Branch agencies and which I help lead in support of the Secretary of the Treasury's role as Chair—carefully reviews foreign investments in the United States for national security risks. When necessary, the Committee takes action to address any such risks while seeking to maintain an open investment environment and the status of the United States as one of the world's top destinations for foreign direct investment.

CFIUS protects national security in the context of foreign direct investment from *any* country. By law, the Committee analyzes the facts and circumstances of each transaction on a case-by-case basis following a rigorous review process that leverages subject-matter expertise across the Executive Branch. Our risk analysis is focused on three factors: the threat emanating from the foreign investor, the national security vulnerabilities presented by the U.S. business, and the consequence of a transaction to national security. When we identify a risk, our mandate is to

resolve it, whether by mitigating the risk through enforceable restrictions on the parties or, as a last resort, by recommending the President block or unwind a transaction.

Over the years, as national security threat environment has evolved, so has CFIUS. First established by executive order in 1975, the Committee has benefited from congressional action to codify and enhance its authorities. Most recently, Congress did so with the bipartisan Foreign Investment Risk Review Modernization Act of 2018, or FIRRMA. Among other things, FIRRMA provided the Committee with important authorities over certain investment structures that had previously fallen outside its jurisdiction and modernized our processes to better enable timely and effective reviews of covered transactions. It also provided the Committee with much needed jurisdiction over certain transactions involving real estate in close proximity to sensitive facilities.

Treasury has dedicated significant time and resources to the successful implementation of FIRRMA and the efficient processing of what is now an all-time high caseload. Prior to enactment, the Committee processed 237 filings in 2017. Four years later, our case load nearly doubled to 436 filings in 2021. We expect the number of cases to continue at this heightened level.

Since I was confirmed to my role as Assistant Secretary for Investment Security, I have been focused on making sure CFIUS operates effectively and efficiently, bringing to bear all available resources and tools to support our important national security mission. This effort includes the issuance of the first Executive Order since the Committee was established to provide formal Presidential direction on additional risks that we are to consider when reviewing a covered transaction. It also includes the issuance of our first ever enforcement and penalty guidelines to ensure that transaction parties are held accountable for failing to comply with our laws or for not upholding their obligations to mitigate national security risk. While Congress rightly put in place strict confidentiality for information filed with CFIUS, we have and will continue to take enforcement actions on specific matters to protect national security. We are also enhancing our tactics and techniques to ensure we are gathering more detailed information about foreign acquirers and deal structures to thoroughly assess the national security risks arising in any given transaction.

When CFIUS reviews a transaction that raises national security concerns, the Committee can mitigate the risk by requiring that certain measures be undertaken, and these measures are formalized in what we call a National Security Agreement, or mitigation agreement. When we negotiate a mitigation agreement, our work does not stop after the agreement is signed.

We routinely conduct site visits, collect documents and information, and engage with third party monitors and auditors to ensure that the terms of these agreements are upheld and parties live up to their compliance obligations. While preventing violations from occurring is our primary focus, the availability of robust remediation and enforcement tools in the event of non-compliance is necessary because a breach could harm national security. Under the Defense Production Act, the Committee has its own enforcement authority—including subpoena authority—and can impose monetary penalties and seek other remedies for violations of its statute, regulations, mitigation

orders, conditions, or agreements. We will not hesitate to take enforcement action when necessary to protect national security.

We also continue to enhance our ability to identify non-notified transactions and engage with international partners and allies. Indeed, the Committee actively monitors investment activity and follows up on tips from the public and other sources to identify these types of transactions that may pose national security risk. Should we identify a potentially covered transaction that may raise national security concerns, we request the parties file a notice, and initiate our formal review process. We have also established a process to assist partners and allies with foreign investment review—including the sharing of threat information—while contributing to the establishment and modernization of over 20 international foreign direct investment screening mechanisms.

Finally, as we protect national security in the context of inbound investments, we continue to contribute to interagency discussions regarding policies to restrict certain U.S. outbound investments in specific sensitive technologies with significant national security implications. Our desire is to avoid situations in which U.S. investments support and advance technologies that enhance military or intelligence capabilities in countries of concern that could undermine our national security and put Americans at risk.

While we are proud of the Committee's efforts, our work remains unfinished, and there are always ways to improve. We remain focused on being as effective as we can be in our national security mission. You have my commitment that we will use all authorities available to us to protect the national security of the United States.

In the end, as we work to counter the national security risks that emanate from China, as Secretary Yellen has said, where possible we need to find a way to work together for the benefit of the world, but in doing so we never compromise our national security. Thank you again for the opportunity to appear before you today, I look forward to answering any questions you may have.