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 House Select Committee on the Chinese Communist Party (CCP)
Hearing Entitled, "The Biden Administration's PRC Strategy"

July 20, 2023

Chairman Gallagher, Ranking Member Krishnamoorthi, distinguished members of the Select Committee, thank you for inviting me to testify about the ongoing efforts of the Commerce Department, Bureau of Industry and Security's (BIS's) Export Administration 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.

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 our 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, coordinating with our allies and partners on export 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 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. I will also touch on some of the important work of BIS's Export Enforcement to ensure compliance with U.S. export controls and to help deny the PRC unauthorized access to U.S. technologies.

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 when reviewing the transaction details articulated in the export license application is the risk of diversion of the technology 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. As evidenced by these 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, proprietary, and classified information to protect U.S. national security and foreign policy interests 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 by Commerce and its interagency partners. 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 denial 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 the Senate Banking Committee in July of last year, "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 advanced computing items and supercomputing capability, which can support artificial intelligence (AI) applications, as well as semiconductor manufacturing equipment.

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 related to advanced semiconductor production, 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 national security 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 over 700 PRC parties on our Entity List – over 230 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. 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. Concerning PRC Measures

BIS is closely monitoring recent actions taken by the PRC against U.S. semiconductor company Micron, as well as export control measures taken by the PRC on semiconductor-related materials gallium and germanium.

The PRC's recent actions follow a history of state-directed intellectual property theft, forced technology transfers, massive state support of industry, and prejudicial regulation--all designed to enable the PRC to not only undercut global competitors but drive them out of the marketplace. We have seen the PRC do this in a wide range of industries, from batteries to solar to telecommunications.

I saw evidence of such activities first-hand when I prosecuted economic espionage cases at the Department of Justice. The PRC has used this strategy in semiconductors for nearly two decades, including the example of Fujian Jinhua, a PRC state-owned memory chipmaker that was placed on BIS's Entity List following its theft of U.S. intellectual property, which threatened the long-term economic viability of U.S. suppliers of these essential components of U.S. military systems.

The United States and its allies and partners use export controls to address clearly articulated national security and foreign policy concerns. The PRC's actions are inconsistent with its assertions that it is opening its markets and committed to a transparent regulatory framework. Accordingly, we would be concerned that these measures were taken solely as retaliation in the wake of prior export control actions related to semiconductors and a recent announcement by G7 leaders to launch a Coordination Platform on Economic Coercion. The U.S. and our allies and partners use export controls to address legitimate national security and foreign policy concerns, including protection of human rights, and BIS has been transparent through our rulemaking and in public statements about the factors that led us to adopt narrowly targeted controls.

Such coercive and non-transparent measures targeting U.S. and other foreign businesses reinforce the need to diversify and build resilience in our supply chains and to de-risk operations based in the PRC. The Commerce Department has been engaging with several U.S. companies that have been affected and Secretary Raimondo raised her concerns directly with her Chinese counterpart Minister Wang at their most recent meeting in May of this year. We are working to respond to these and other

predatory actions by the PRC through ongoing engagement with allies and partners, as illustrated by the recent G7 statement standing up against the PRC's coercive practices.

VI. 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 38 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 and foreign policy rationales underpinning our controls.

VII. Export Control Enforcement

In addition to the robust export control authorities that BIS's Export Administration exercises, ECRA also provided my colleagues in Export Enforcement with powerful administrative and, in conjunction with our colleagues at the Department of Justice, criminal enforcement authorities. Under the leadership of Assistant Secretary for Export Enforcement Matthew S. Axelrod, Export Enforcement has leveraged its investigative tools and interagency partnerships to aggressively enforce 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.

For example, 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. Since that rule and implementation of a memorandum outlining a two-step policy to address persistent scheduling delays of our end-use checks, we have completed over 90 end-use checks in China. Prior to this policy change, the Chinese government had not allowed us to conduct a check in over two years.

To complement my team's focus on advanced technology sectors, in February 2023, Export Enforcement and the Department of Justice National Security Division formed the Disruptive Technology Strike Force. 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. This includes leveraging the authorities and resources of DOJ, the FBI, Homeland Security Investigations, and BIS in 14 cells across the United States along with a DC-based analytical cell. This past May, BIS and DOJ announced the first wave of Strike Force enforcement actions, including arrests, indictments, and a temporary denial order in five different cases across the country involving China, Russia, and Iran.

Export Enforcement also is aggressively penalizing violators. For example, this past April, BIS 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 without a license after BIS's imposition of the Huawei Foreign Direct Product Rule. It is also the first enforcement case and penalty brought under the Huawei Foreign Direct Product Rule since that rule was issued in August 2020. Seagate is also 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.

Like Export Administration, Export Enforcement is collaborating with enforcement partners internationally to identify and address export evasion risks and enhance their ability to prevent unauthorized transfers and safeguard collective national security interests. This includes bilaterally through its Export Control Officers program, which includes two officials stationed in Beijing and Frankfurt, and one each in Dubai, Hong Kong, Istanbul, New Delhi, and Singapore, with three new posts opening this summer in Ottawa, Helsinki, and Taipei; and multilaterally, for example, with Five Eyes partners from Australia, Canada, New Zealand, and the United Kingdom as announced in June, as well as with G7 partners along with the European Commission.

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.