UNITED STATES DEPARTMENT OF COMMERCE
Under Secretary for Industry and Security
Washington, D.C. 20230

Statement of
Alan F. Estevez
Under Secretary of Commerce for Industry and Security
Before the House Committee on Foreign Affairs
Hearing Entitled:
"Countering China on the World Stage: Empowering American Businesses and Denying Chinese Military Our Technology"
Thursday, March 21, 2024

Chairman McCaul, Ranking Member Meeks, members of the Committee, it is my honor to testify before you today.

This morning, I want to start by framing how export controls fit into our current era of strategic competition.

I will touch on our actions to respond to Russia's brutal invasion of Ukraine, which is a real-world case study in the application of export controls to a new and fast-moving threat landscape. Then I will describe the evolution of our controls on the People's Republic of China (PRC), including our enforcement work.

Finally, I will address what the Committee can do to ensure that the Bureau of Industry and Security (BIS) remains a dynamic asset for national security in the digital age.

Export Controls in an Era of Strategic Competition

As the National Security Strategy and Intelligence Community's Annual Threat Assessment make clear, we are in an era where competition from nation-states—particularly the PRC, Russia, Iran, and the Democratic People's Republic of Korea (DPRK)—is intersecting with cross-cutting global challenges. As a result, more domains are being contested. This, combined with the proliferation of new and powerful commercial technologies, is enabling new and different threats.

As the Committee is well aware, items and technologies such as semiconductors, unmanned aerial vehicles (UAVs or drones), and information and communications technology and services (ICTS), are reshaping the security environment. Russia is employing inexpensive but deadly drones, including those developed by and acquired from Iran, against Ukraine. The Chinese Communist Party (CCP) is seeking to develop and use supercomputing capabilities, as well as developing artificial intelligence (AI) capabilities, for a host of military modernization activities and human rights abuses. The DPRK is well known to pursue cybercrime and other malicious activities via the internet. All of these actors are engaged in internet-based mis- and disinformation activities, including through apps used by millions of Americans every day.

In other words, as our nation seeks to continue to innovate and benefit from technological advancement, we also have to be careful not to create new areas of vulnerability—and to work hard to secure those that do exist.

That is what we are focused on at BIS. Our mission is to protect U.S. national security and foreign policy interests, and to advance U.S. technological leadership. We have operated for decades at the nexus of national security, technology, and commerce. However, given today's threat environment combined with rapidly evolving commercial technology and innovation, our tools are being called on increasingly in to protect national security.

BIS's work has become more central to the U.S. Government's overall strategic toolkit. Export controls are a strategic tool for denying foreign adversaries access to dual-use commodities, software, and technology, and in certain cases, even U.S. services, that can support military applications and human rights abuses. They are not the silver bullet or only tool needed to address the national security threats that emanate from the technology sector, but they are a significant force multiplier when coupled with diplomatic engagement, sanctions, domestic investments in U.S. capabilities, and other tools.

Supply chains, particularly for advanced technologies, are global. The PRC and other countries of concern have certain indigenous capabilities that are close to comparable, or are comparable, with U.S. and allied capabilities, which can be used to undermine our national security. To maintain our advantages, we must work to keep pace through refining and updating our controls. We must also work vigorously to bring more international partners to the table. This helps to ensure that our adversaries are denied U.S. technologies, as well as comparable technologies produced by other countries, that present national security concerns. There is no magic export control that the U.S. can impose alone that will permanently stop malign actors—therefore, our work is never done, and we are constantly vigilant.

Ultimately, BIS's work is what the military sometimes refers to as a "Phase Zero" operation—continuous daily work to continue building relationships with partners and allies, while we stay on top of technological developments, and security threats. Our goal is to help shape the overall security environment as advantageously for the U.S. and our allies as possible.

To do that, BIS needs to keep pace with real-world technological, commercial, and geopolitical events and actions—and we have.

Under the Biden-Harris Administration, export controls have been used in a deliberate, strategic, and effective manner to confront the threats we face today, and to shape the security environment for the future.

Russia

As the Committee knows, since February 2022, BIS has responded to Russia's full-scale invasion of Ukraine by imposing sweeping controls on a host of items—as well as adding over 900 end-users in Russia, Belarus, the PRC, Iran, and more than 30 other countries to the Entity List.

We worked quickly alongside our interagency partners to build a coalition of the United States and 38 international allies and partners that are imposing substantially similar controls. This multilateral approach was critical as the U.S.-Russia volume of trade was relatively small at the start of Russia's further invasion of Ukraine.

As a result of extensive efforts by the United States and its partners, worldwide exports to Russia since its February 2022 invasion have fallen approximately 29 percent (an average of $7.1 billion per month) by value, compared to the same period preceding the invasion.

From February 2022 to January 2024, U.S. exports to Russia of all products have fallen approximately 88 percent (an average of $471 million per month) by value. Our limited remaining trade is concentrated in medical items such as vaccines.

From February 24, 2022, to December 31, 2023, the law enforcement arm of BIS, the Office of Export Enforcement (OEE), detained 559 shipments that were destined to Russia, valued at over $284 million. In that time period, OEE prevented 206 shipments, inspected 132 shipments, ordered 20 shipments redelivered, and seized 105 shipments. Many of the investigations involved schemes to purchase critical dual-use technology to include military grade components that could be used in missiles and UAVs; some of which were found in Russian weapons platforms and signals intelligence equipment recovered from the battlefield in Ukraine. BIS also leveraged its administrative authorities to include Temporary Denial Orders (TDOs) to prevent imminent violations of U.S. export control laws and published a public list of Russian and Belarusian airlines that violated Export Administration Regulations.

These actions have imposed increased costs on the Kremlin in a host of areas and forced Russia to rely on international pariah states like Iran and the DPRK for weapons. BIS's actions have forced the Russians to turn to the PRC and non-aligned countries to sustain their economy.

The export controls imposed by the United States and our allies and partners will continue to erode Russia's military capabilities over the long-term. The lower capability dual-use items they have resorted to procuring do not substitute for more advanced components —and we are working hard to crack down on illicit networks that they are seeking to build to obtain what they really want. Last month, for example, a Russian citizen pleaded guilty in federal court to charges of money laundering and smuggling for operating a procurement network that fraudulently obtained from U.S. distributors large quantities of dual-use, military grade microelectronics, specifically OLED micro-displays, on behalf of Russia-based end users.

We will continue working with the interagency partners and internationally on alignment and enforcement of controls. We are working with industry on ways to enhance due diligence, working vigorously with allies and partners to identify efforts to evade and disrupt our controls, and leveraging our unique enforcement tools combined with the support of our interagency partners to aggressively investigate and penalize violators.

However, I want to be clear: the United States needs to continue funding to support Ukraine in its fight and use all of the other tools in our toolkit to continue to impose costs on Russia and those that seek to support it.

The PRC

Our relationship with the PRC is very different from that with Russia. We have substantial trade with the PRC across a variety of sectors—on the order of $700 billion in goods trade per year. It is the world's second largest economy. The PRC has the intent and increasing capacity to project power across a variety of domains, both geographic and strategic.

Many of our allies and partners also have significant relationships with, and in some cases, reliance on the PRC.

Therefore, the strategic choices and security challenges presented by the PRC are different than in other cases, including the Russia case.

For decades, the United States has had export controls on trade with the PRC for multilaterally controlled items. We also have an arms embargo in place and controls on a host of other items. All of these controls remain in place today.

Over the past several decades, the PRC has sought to build and now weaponize their industrial capacity and unfair, non-market-oriented economic policies and practices to gain strategic advantage. They have pursued a "Military-Civil Fusion" strategy and spent hundreds of billions of dollars to carry out their state-directed industrial targeting goals, including in the semiconductor sector. The U.S. application of export controls to address these national security threats began to intensify in 2018.

Since 2019, BIS has taken several actions, including updating licensing policies for Hong Kong and expanding controls related to military end users in the PRC. T the U.S. government also took unilateral export controls actions against major PRC companies by adding them to the Entity List. In part because of the size and scope of these enterprises and their importance in global supply chains, the restrictions put in place at the time on certain entities were not absolute, and allowed certain exports of items that met the criteria outlined in the listings to continue with U.S. government authorization. There were not comparable actions by key international allies.

I want to be clear: Any approvals of licenses for these entities, regardless of Administration, follow the restrictive rules established by the interagency process, which includes review by the Departments of State, Defense, Energy, and Commerce and were consistent with the policies outlined in the Entity Listings. As almost any export transaction with an Entity Listed party requires a license, exporters sought licenses for a wide range of items, including office supplies like printers and similar items that the interagency review process concluded did not pose national security risks. The actions taken impacted the targeted companies in the way the controls were intended. However, export controls are not static, and the limitations of a unilateral approach have become clear, and the actions taken during the Biden-Harris Administration have built on and improved the regulations developed over the years.

First, we have imposed PRC-wide restrictions on advanced semiconductors, semiconductor manufacturing equipment, the services that can be provided by U.S. persons, and other related items. This country-wide approach is important because we are clearly identifying a strategic sector and strategic items, and setting clear lines based on technological capabilities. This is also a much more durable and effective approach for stakeholders and industry to understand and comply with than relying on case-by-case license reviews. We are already seeing reports of constraints within the PRC's high-performance computing capacity, suggesting that they are facing difficulties in obtaining and producing the necessary advanced chips due to our restrictions.

Second, over the course of the past year, key allies and partners have imposed substantially similar controls on advanced semiconductor manufacturing equipment. Supply chains, particularly for advanced semiconductors, are global and not only the PRC but also many other countries play important roles in the sector. The United States is vigorously working to strengthen our partnerships and coordination with those key allies and partners—while also seeking to bring on others—to

further clamp down on the PRC's ability to obtain a broader range of items and support that it needs to enhance its military capabilities.

Along those lines, it has been encouraging to see allies and partners recognizing the threat the PRC and others pose and taking appropriate actions to address security concerns regarding semiconductors and other emerging technologies, through their domestic legal systems. For instance, France recently put in place controls on quantum computing and semiconductor technologies. The United Kingdom has announced additional controls on quantum and semiconductor technologies, among other sensitive items. In addition, it has been reported that key South Korean firms intend to no longer sell used semiconductor manufacturing equipment into to the PRC. Also, the governments of the Netherlands and Japan have announced and implemented controls on semiconductor manufacturing equipment.

Third, we continue to be vigilant in identifying PRC end-users of concern and adding them to the Entity List as appropriate. There are now over 800 PRC entities on the Entity List, including more than 300 added in this Administration. These actions help to backstop our item-based, country-wide controls and provide an important and flexible tool for denying PRC entities access to items for military applications and human rights abuses.

Fourth, we are working to use our other authorities alongside export controls to enhance both our work and the work of our interagency partners. For example, we are using our industrial base survey authority to implement portions of the President's AI Executive Order, and also to provide critical insight into the U.S. supply chains for legacy chips from the PRC. BIS is also exercising its ICTS supply chain authorities, including through beginning the rulemaking process to investigate the national security concerns presented by connected vehicles from the PRC and other countries of concern. These authorities enhance BIS's mission and will continue to be formidable tools.

Finally, the Administration is not relying on BIS tools alone. The Department of Commerce is also administering the CHIPS Act of 2022. This law incentivizes investment in semiconductor facilities and equipment in the United States to provide a secure supply of semiconductors for national security and critical infrastructure, and to support the technology leadership of the United States. Awards under the CHIPS Program are also subject to national security guardrails intended to ensure that funding provided through this program does not directly or indirectly benefit foreign countries of concern, including the PRC. Commerce is also administering important investments and programs under other key laws enacted during this Administration. Other Departments are similarly focused on strategic competition with the PRC and are engaged in using their authorities and resources as well. By taking a whole-of-government approach to strengthening and enhancing our capabilities here at home and also working to coordinate with allies and partners, we are making it more likely that export controls will have an even greater strategic impact in the future.

Expanded Controls Require Enhanced Enforcement

Effective enforcement is a critical factor in the success of export controls as a strategic asset, and BIS has worked hard to update its policies for maximum impact, leverage partnerships internationally and across the federal government, and prioritize our limited resources effectively.
BIS remains laser-focused on preventing sensitive U.S. technologies and goods from being used for malign purposes by our adversaries. That is why we established the Disruptive Technology Strike Force in partnership with the Department of Justice last year. The Strike Force brings together experienced agents and prosecutors in seventeen locations across the country, supported by an interagency intelligence effort in Washington, DC, to aggressively pursue enforcement actions

against illegal procurement networks and prevent nation-state actors from illicitly acquiring our most sensitive technology. In the year since the Disruptive Technology Strike Force's formation, for example, the Strike Force has successfully charged 14 cases involving alleged sanctions and export control violations, smuggling conspiracies, and other offenses related to the unlawful transfer of sensitive information, goods, and military-grade technology to Russia, the PRC, or Iran. Specifically, three cases charged former employees of U.S. companies with stealing confidential and proprietary information related to sensitive technology and attempting to take such information to the PRC, and one case charged a defendant with seeking to obtain technology from U.S. manufacturers on behalf of PRC end users.

Additionally, earlier this month the Strike Force charged a former Google engineer with theft of trade secrets in connection with an alleged plan to steal from Google LLC proprietary information related to AI technology and provide it to two companies based in the PRC.

The Strike Force's work has also led to the issuance of Temporary Denial Orders against 29 entities, including airlines, freight forwarders, defense companies, and others to cut off their access to controlled U.S. items, and contributions to numerous parties being placed on Commerce's Entity List and Treasury's Specially Designated Nationals and Blocked Persons List.

The Strike Force has also forged international partnerships committed to preventing critical technology from being siphoned off by foreign adversaries and has fostered partnerships with the private sector, working directly with companies involved in the manufacture, sale, and shipment of sensitive export-controlled items, through industry outreach events, roundtables with stakeholders, and other efforts.

With respect to the PRC, in addition to the Strike Force cases already referenced, we have taken—and will continue to pursue—targeted, aggressive action to enforce our rules.

On October 7, 2022, 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. We established a policy with a two-step process to address persistent scheduling delays of our end-use checks. Under the policy, if BIS requests an end-use check by 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 will initiate the regulatory process with our interagency partners to place the unchecked company on the Entity List. Prior to this policy change, the PRC government had not allowed us to conduct a check in over two years. This policy led directly to improved cooperation with our pending checks. In the year since the policy was announced, we have completed over 130 end-use checks in the PRC. End-use checks are an important tool for compliance with export controls, but they are not the only factor—we make sure to corroborate against all-source intelligence, and retain substantial authorities to halt shipments and take other actions if appropriate.

In 2023, we issued our largest standalone civil penalty in history of $300 million on Seagate Technologies, LLC., for alleged violations of U.S. export controls related to selling hard disk drives to Huawei Technologies Co. Ltd. even after Seagate's only two competitors had stopped sales because of the foreign direct product rule.

In January 2024, four PRC nationals were charged with various federal crimes related to a years-long conspiracy to unlawfully export and smuggle U.S.-origin electronic components from the United States to Iran that would ultimately benefit entities affiliated with the Islamic Revolutionary Guard Corps and Ministry of Defense and Armed Forces Logistics which supervises Iran's production and development of weapons, missiles, and UAVs.

BIS will continue building on these critical actions in the coming year.

Export Controls are a Strategic Tool—That Needs Continued Support and Investment

The current era of strategic competition is dynamic. The United States is contending with a host of national security threats posed by nation-states and exacerbated by rapid technological advancement. The Biden-Harris Administration has been navigating those challenges by reinvigorating our multilateral efforts, and by employing national security tools like export controls in new ways. BIS has been asked to do more in an era of strategic competition where economic statecraft is increasingly central to U.S. interests and strategy. We have risen to every challenge that we have been asked to take on.

However, to sustain our current pace and effectiveness, there are a few realities that the Committee should consider:

- BIS's budget for core export control functions has remained essentially flat since 2010, when adjusted for inflation.
- BIS' law enforcement arm, OEE, employs only 150 agents to counter the threat posed by nation state actors, which means an increase in sworn law enforcement officers and analysts is overdue.
- Total U.S. exports are up approximately 62 percent since 2010, and exports subject to BIS license requirements are up approximately 126 percent since 2014.
- Our licensing workload has doubled from approximately 20,000 per year in 2012, to over 40,000 per year.
- Our staff are relying on foundational systems for both license adjudication and enforcement work that were put in service in 2006 and 2008, respectively.
- License review timelines continue to increase, particularly to the PRC, as licenses become more complex, particularly for exports of electronic components.

Notwithstanding these challenges, we achieved an all-time high in the number of criminal convictions and months in jail, resolved or imposed the highest number of administrative cases, denial orders, and temporary denial orders, and conducted a record 1,500 end use checks globally in fiscal year 2023.

As you can see, BIS's staff has been asked to do more with less for a long time, and yet our results are impressive.

We hope to continue constructive work with the Committee to ensure that BIS has the resources and policy support needed to continue its mission-critical work.

Supporting the President's Budget for Fiscal Year 2025 is an important step that will allow us to sustain the robust, effective efforts we have underway, particularly with respect to PRC.

BIS is committed to protecting U.S. national security, and we will continue to up our game to keep pace with ever-changing security threats generated by the geopolitical and technological environment.

I look forward to your questions.

###