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.