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 Foreign Affairs Committee

July 19, 2022

Chairman Meeks, Ranking Member McCaul, members of the Committee, thank you for inviting me to testify today on the work of the Commerce Department's Bureau of Industry and Security, or BIS.

BIS's mission is to advance U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership.

We execute this mission by imposing appropriate controls on exports and reexports of lower-capability military items, dual-use items (i.e., those items having both commercial and military or proliferation applications), and predominantly commercial items. We have the authority to seek criminal and administrative sanctions when appropriate for violations of our export controls. We also play an important role in Commerce's analysis and support of our industrial base, and the Department's participation on the Committee on Foreign Investment in the United States (CFIUS).

Put another way, our primary goal is to prevent malign actors from obtaining or diverting items, including technologies, for unauthorized purposes, in order to protect our national security and advance our foreign policy objectives while supporting the competitiveness of our key industries.

BIS's mission has never been more relevant. We face ongoing national security threats from nation states—China, Russia, Iran, North Korea—as well as from terrorists and other non-state actors. However, on top of the traditional threats posed by those actors, we also must contend with an evolving threat landscape and the use of commercially available technologies to further activities of concern, including human rights abuses.

As Under Secretary of Commerce for Industry and Security, I view my role as the "Chief Technology Protection Officer" of the United States. BIS operates at the nexus of national security and technology, and export controls are a unique and powerful tool for responding to the modern threat environment that we face. This is particularly true when we work together with our allies and partners.

We are in an important moment for our national security, and today I will focus on BIS's role administering and enforcing export controls to address four critical challenges: first, our response to Russia's further invasion of Ukraine; second, the pacing threat that China represents; third, the identification of emerging and foundational technologies essential to national security; and finally, the need to build a durable, multilateral technology security framework for the future use of export controls.

Responding to Russia's Further Invasion of Ukraine

BIS has robust authorities under the Export Control Reform Act of 2018, or ECRA. Using those authorities, BIS has imposed sweeping export controls on Russia for its unjustified, unprovoked, and premeditated further invasion of Ukraine, and on Belarus for its substantial enabling of that invasion. And thanks to the additional resources Congress provided to BIS in the Ukraine Fiscal Year (FY) 2022 supplemental spending bill, we are prepared to sustain and expand those actions against Russia and Belarus.

Our goal is to choke off exports of technologies and other items that support Russia's defense industrial base, including defense, aerospace, and maritime sectors, and to degrade Russia's military capabilities and ability to project power. While the impact of our export controls will only increase over time as Russia is unable to repair, replace, and replenish its military hardware, we are seeing substantial impacts of our actions in the data available to date:

- Since the start of the invasion on February 24 through July 1, 2022, U.S. exports to Russia in categories of items subject to new U.S. export license requirements decreased by 95.9 percent by value as compared to the same period in 2021.

- Overall U.S. exports to Russia have decreased by approximately 88 percent by value over the same period in 2021 (February 24-July 1, 2021).

- Analysis of trade data conducted by the Peterson Institute for International Economics (PIIE) shows that, of the 54 countries that make up approximately 90 percent of Russia's imports, those with similar export controls against Russia in place have seen total exports to Russia decline by a cumulative 60 percent since the invasion. Exports to Russia from countries that have not imposed similar controls are also down 40 percent.

- PIIE goes on to point out that "the inaccessibility of foreign tech and components is hitting Russia's maintenance; supply; and future development of chips, guided missiles, tanks, cars, planes, and much more. Russia's own economy ministry is projecting a GDP contraction of up to 12.4 percent in 2022."

There are numerous open-source reports on the need for Western semiconductors as key inputs to Russian weapons systems. Since our controls have fully taken effect, there has been a 74 percent reduction by value of global exports of semiconductors to Russia compared to the same period in

2021 (March-May). This has prompted Putin himself to issue public concerns about where Russia will source these critical inputs.

We have also taken multiple actions that have impacted Russia's aerospace sector, which is reliant on U.S. and European manufactured planes, parts, and service necessary to maintain them. There have been reports that Russia will have to ground between half and two thirds of its commercial fleet by 2025 in order to cannibalize them for parts due to the export controls and enforcement actions we have implemented. And as our recent Entity List actions demonstrate, where we identify companies that attempt to backfill our restrictions, we will take swift action.

These are just some examples of the impact our controls are having to date. This is one of the most aggressive and robust uses of export controls against another country, and these impacts would not be possible without the unprecedented level of coordination with our allies and partners around the world.

While there is an appropriate role for unilateral export controls, as Congress noted in ECRA, "[e]xport controls that are multilateral are most effective[.]" If other countries supply the same types of items that the United States restricts, the U.S. controls will be ineffective for two reasons. First, the countries or parties of concern will still acquire the items at issue. Second, U.S. technology leadership will be threatened if foreign competitors can undercut U.S. companies and earn revenue to invest in research and development. Thus, coordinating with allies and partners also helps keep a level playing field for U.S. companies and helps maintain U.S. technology leadership and competitiveness, all of which contribute to national security, as described in ECRA.

Thanks to the hard work done by the Biden Administration—from the President on down—we have built a coalition of 37 other countries so far who have agreed to adopt substantially similar controls on Russia and on Belarus.

Our message to countries that have not joined our restrictions on exports to Russia is that if they share our horror at Russia's aggression against Ukraine and our respect for the rule of law, they should join the United States and our partner countries around the Indo-Pacific and Europe in imposing stringent restrictions on exports to Russia.

To maximize the effectiveness of our controls, we have conducted extensive outreach to the public to educate them on the changes. BIS conducts regular outreach to the exporting community to inform and share best practices, and utilizes international partnerships to educate foreign companies about U.S. export controls. Since February 24, we have conducted outreach on the new controls to over 3,000 entities and individuals.

In addition, we are aggressively enforcing the new controls. We deploy a variety of resources and tools to ensure effective enforcement, including leveraging relationships with other law enforcement agencies, the Intelligence Community, and international partners. BIS conducts physical inspections (e.g., end-use checks and port inspections/detentions) to detect illicit

procurements, and we investigate potential violations of U.S. export controls and, if appropriate, vigorously pursue criminal and civil penalties. Since Russia's further invasion of Ukraine on February 24, we have detained or seized 218 shipments valued at $90 million.

Related to my earlier statements about Russia's deteriorating commercial aviation industry, we have tracked and publicly released a list of over 150 aircraft that we believe operated in violation of our Russia and Belarus controls, in order to provide notice to the world that servicing these aircraft is itself violative of our rules. We also recently issued our first public charging letter against Russian oligarch Roman Abramovich related to his improper export of two private planes, alongside a seizure warrant for the planes obtained by the Department of Justice. We have issued nine temporary denial orders, or TDOs, against various Russian airlines, which effectively cut off not only their right to export items subject to our regulations from the United States, but also their right to receive or otherwise participate in exports from the U.S. of such items.

The Pacing Challenge: China

As we continue our robust response to Russia's further invasion of Ukraine, we remain focused on aggressively and appropriately using our tools to contend with the long-term strategic competition with the People's Republic of China (PRC).

The PRC threat to our national security and foreign policy interests is real. My north star at BIS as it relates to China is to ensure we are appropriately doing everything within our power to prevent sensitive technologies with military applications from getting into the hands of China's military, intelligence, and security services.

Export controls are at the forefront of the many tools that the Biden Administration is using to coordinate and respond to China's destabilizing activities. We are using our controls to address China's military-civil fusion strategy that seeks to divert dual-use technologies to military uses, military modernization, WMD program development, human rights abuses, and efforts to destabilize the Indo-Pacific region. Confronting these actions protects our national security and advances our values and interests, as well as those of our allies and partners. This is a dynamic threat environment, and we are constantly evaluating our existing authorities and thinking about how we can employ our tools to maximum effect.

We continue to maintain comprehensive controls related to the PRC, including requiring a license for: all military and spacecraft items under our jurisdiction; 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; and all items under our jurisdiction, if the item is exported knowing it will be used in certain WMD programs or if it is intended, entirely or in part, for military-intelligence end uses or end users in China. In addition, the Export Administration Regulations (EAR) prohibit certain U.S. person activities that would support WMD-related activities or military-intelligence end use or end users in China absent authorization. Thus, the EAR's licensing requirements for China seek to prevent

activities that threaten U.S. national security and foreign policy interests while allowing commercial activities that do not raise such issues.

We also use our Entity List to identify parties of concern, many of whom are subject to license requirements for all items under our jurisdiction, regardless of the sensitivity of the item. Currently, we have nearly 600 Chinese parties on our Entity List – 107 of those added during the Biden Administration. These parties have been added for a variety of reasons ranging from supporting China's military modernization and WMD programs, to supporting Iran's WMD and military programs, to facilitating human rights abuses in Xinjiang. These parties include those involved in artificial intelligence, surveillance, biotechnology, and quantum computing.

We are continually assessing available open-source, proprietary, and classified information, in coordination with our interagency partners, for the addition of other parties to the Entity List and other restricted party lists maintained by BIS in connection with the enabling of China's military-civil fusion strategy and other malign activities.

Addition to the Entity List means that anyone seeking to export or transfer items under Commerce jurisdiction to a listed party must first seek a license to do so from Commerce. As with all license applications, those applications are generally reviewed by the Departments of Commerce, State, Defense, and Energy. As a general matter, such license applications for parties on the Entity List are reviewed under a presumption of denial. For those 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 transactions that may be approved by the interagency process.

In the select instances where there is disagreement among the agencies on whether to approve the license, there is an established process for any agency to initiate further escalation and review. During FY 2021, only 0.14% of all applications submitted were appealed to the Assistant Secretary level. While the agencies may have different perspectives on individual cases, we all bring helpful expertise to the process and can reach accommodation on almost all applications. And when we cannot, the interagency review and escalation process forces us to bring our best arguments to the table to help shape U.S. export control policy.

In addition to the Entity List, we also maintain the Unverified List, which includes parties for which we cannot verify their *bona fides* (*i.e.*, legitimacy and reliability relating to the end use and end user of items subject to the EAR). Earlier this year, we added 33 Chinese parties to the Unverified List as BIS was unable to verify their *bona fides* because an end-use check could not be completed satisfactorily for reasons outside the U.S. Government's control. Because of this designation, no license exceptions can be used to export to these parties, and BIS is imposing a pre-license check for any license application involving these parties.

We know that the PRC is determined to advance its military capabilities by illicitly acquiring U.S. technology. Our enforcement team at BIS is dedicated to preventing this from happening by

utilizing all of our criminal and administrative investigative tools, as well as regulatory actions like the Entity List and Unverified List, to aggressively enforce our export control rules.

For example, 21% of the Office of Export Enforcement's current investigations involve China as the ultimate destination. And in FY 2021, 66% of criminal penalties and 40% of administrative penalties levied related to export violations involving China, totaling almost $6 million, as well as resulting in 226 months of incarceration. In addition to monetary penalties, we also have a powerful administrative tool to deny export privileges. For example, in June, we imposed a temporary denial order on three interrelated companies – Quicksilver Manufacturing Inc., Rapid Cut LLC, and U.S. Prototype Inc – that contracted with U.S. defense and aerospace customers to 3-D print items based off sensitive prototype space and defense technologies. The three companies illegally sent the blueprints and technical drawings to China to create 3-D prints, which were then shipped back to the United States. BIS's action prevents these three companies from participating in, or benefiting from, any export transaction while our investigation continues.

China remains a complex challenge in the competition between democracies and autocracies. We continue to assess the effectiveness of our controls to address our national security and foreign policy concerns related to the PRC and analyze whether the current threat landscape requires new action. We are closely reviewing our approach to China, seeking to maximize the effectiveness of our controls.

Identifying Emerging and Foundational Technologies Essential to National Security

One such assessment is our continuous review to identify emerging and foundational technologies essential to the national security of the United States, as required under Section 1758 of ECRA. As many of you know, this topic has attracted considerable attention, and for very good reason. BIS works closely with our interagency colleagues to stay informed on new technologies with national security implications and determine whether we need to recalibrate controls on new or existing technologies subject to our jurisdiction. Since enactment of ECRA, BIS has established 38 new controls on emerging technologies, including controls related to semiconductor production, biotechnology, and quantum computing. All but one of these controls are multilateral, with the one unilateral control pending multilateral agreement.

As part of interagency groups led by the National Security Council, we have finished reviewing seven technology groups, which has contributed to proposing and finalizing new controls. In many cases, these reviews have also found that our current controls were sufficient to capture emerging technology roadmaps. Where updates were needed, we have prioritized updating and adding new controls. In addition, BIS has identified technologies that were also identified through CFIUS filings to propose potential controls on emerging and foundational technologies.

We're also continuing to do more to involve parts of the government that are closer to the development and funding of new technologies. I am working with the Department of Defense Under Secretaries for Acquisition and Sustainment and for Research and Engineering to establish

a critical technologies review board. This board will help BIS to understand the technologies DoD is investing in for military use, and help us provide the appropriate controls for those technologies.

We are also working to propose or implement new controls faster and more efficiently. As part of a May 23, 2022 rule, we informed the public that we would no longer characterize new controls as corresponding to "emerging" technology or corresponding to "foundational" technology, instead referring to the technologies at issue as "Section 1758 technologies." As we noted in that rule, this approach reflects the difficulties in drawing meaningful and functional distinctions between technologies for purposes of fulfilling our statutory obligations under Section 1758 of ECRA. Attempting to do so, without statutory definitions for those terms, resulted in delays in proposing and implementing new controls on such items because there is no clear, consistent agreement within the government and in the public on how to apply the terms "emerging" and "foundational" to specific technologies.

Attempting to characterize a technology as either "emerging" or "foundational" reduces our flexibility to respond to real-time developments in rapidly changing technological landscapes. For example, the marine toxins identified in our most recent proposed rule defy common attempts to define "emerging" and "foundational" as these toxins are naturally occurring items that are not new and have never been on the Commerce Control List. Calling such items "Section 1758 Technologies" maximizes our flexibility and effectiveness. As Under Secretary for Industry and Security, my fundamental principle is that if there is a technology that could potentially harm our national security (and is essential to our national security), we want to assess it and if appropriate, impose controls on it – regardless of whether it can be labeled "emerging" or "foundational."

While we will use the term "Section 1758 Technologies" going forward, we will continue to review whether additional controls are warranted for technologies that may be viewed as "foundational," or "emerging." We are statutorily required to do this. We are also statutorily required to consider three criteria when identifying emerging or foundational technologies: (i) the development of emerging and foundational technologies in foreign countries; (ii) the effect export controls may have on the development of such technologies in the United States; and (iii) the effectiveness of export controls on limiting the proliferation of emerging and foundational technologies to foreign countries. Thus, imposing new, unilateral controls on a technology that foreign suppliers can backfill or that a target country already has would be ineffective and primarily undermine U.S. development of such technologies. That is the key challenge with more mature technologies and raises the importance of obtaining multilateral or plurilateral controls for such items.

Multilateral Cooperation Essential to Our Security

That brings me to the final topic I want to discuss today: furthering multilateral cooperation to more timely address national security and foreign policy concerns.

Given the great work we have done with our partners with regards to Russia, and given the threats posed by China – and other malicious actors in the world – I believe we have been presented with a great opportunity to further coordinate with our allies.

In all the export control policy areas I have described, it is clear that cooperation with allies and partner countries is essential to the effectiveness of these controls. To that end, we are involved in working with various groups, including the European Union in the Trade and Technology Council's Export Control Working Group and Japan in the Japan-United States Commercial and Industrial Partnership. We are also leading an export control effort in the Indo-Pacific Economic Framework for Prosperity.

Additionally, we are working with colleagues across the interagency to lead the multilateral Export Controls and Human Rights Initiative, which we announced during the Summit for Democracy. Through this effort, we are working with foreign government partners to establish a voluntary, written code of conduct around which like-minded states could pledge to use export control tools to prevent the proliferation of software and other technologies used to enable serious human rights abuses.

We continue to monitor the effectiveness of the current multilateral regimes and, when necessary, identify areas of plurilateral cooperation in certain technologies with other supplier countries. All four multilateral regimes maintain key controls in restricting the proliferation of conventional arms, dual-use items, and items related to WMD activities. In addition, to mitigate today's threats, we must also work with like-minded governments of supplier countries of certain technologies of concern, including to identify ways to use export controls to limit the use of technologies to commit human rights abuses.

Finally, enforcement is critical to ensuring effective export controls and we are working with partners across the globe on this effort as well. We recently announced an enhanced export enforcement partnership with Canada, and we are working with the European Commission and its Member States on a similar coordination effort. Our Export Control Officers around the globe are also working with enforcement partners in countries stretching from Europe to East Asia, including Singapore and the United Arab Emirates, to enhance export control enforcement and prevent the diversion of U.S.-origin items.

Ultimately, for the United States to maintain effective export controls and technology leadership, which itself is a part of our national security, we need to work in cooperation with others. Our work with the 37 other countries to implement the Russia controls helps provide a blueprint for advancing further. We have momentum on export controls that I will be working to carry forward as we build a new technology security architecture.

***

We have a lot of work ahead of us on all of these fronts, and there are many more areas where BIS is doing important work that I have not discussed. I am proud to be serving in this critical

moment, and I value the partnership and collaboration with you and your staffs as we tackle these challenges together.

Thank you again for the honor of inviting me here to testify today, and I look forward to your questions.