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 House Foreign Affairs Subcommittee on Oversight and Accountability
Hearing Entitled, "Reviewing the Bureau of Industry and Security, Part II: U.S. Export Controls in an Era of Strategic Competition"

December 12, 2023

Chairman Mast, Ranking Member Crow, 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 nation-state adversaries unauthorized access to U.S. technologies.

I currently serve as the Assistant Secretary for Export Enforcement at the Commerce Department's Bureau of Industry and Security (BIS). When Congress passed the Export Control Reform Act of 2018 (ECRA), it provided my team of law enforcement agents and analysts with robust administrative and criminal enforcement authorities. We now 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 (ODNI) publishes the Intelligence Community's (IC's) Annual Threat Assessment, which details 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 Russia does not appear until page 16. China is not discussed until page 20.

Compare that to this year's assessment and you will see how significantly our national security landscape has changed. While terrorism of course remains a significant and pressing threat, 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 very 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. . . . Iran will remain a regional menace with broader malign influence activities, and North Korea will expand its WMD capabilities while being a disruptive player on the regional and world stages."

Given this evolving 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 China, Russia, Iran, and other nation-state actors – is more critical than at any other time in the organization's history. It is among the reasons why I am so honored to lead such an expert and dedicated law enforcement team at this specific point in time. The team and I work every day to meet this unprecedented moment. More specifically, during my tenure, 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 – including China, Russia, Iran, and other threat actors.

1. *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.

- On June 2, 2022, we promulgated 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 and the public more timely insight into actions that we believe violate our rules. The following week, on June 6, 2022, we published a Charging Letter against Russian oligarch Roman Abramovich, alleging violations of the Export Administration Regulations (EAR) involving flights of two U.S.-origin aircraft to Russia without the required export licenses from BIS.

- On June 28, 2022, we launched a new Academic Outreach Initiative to help academic institutions maintain an open, collaborative research environment in a way that also protects them from national security risk. The effort prioritizes Export Enforcement's engagement with specific academic research institutions whose work gives them an elevated risk profile, such as working with the Department of Defense (DOD) or with parties on the Entity List. The initiative assigns Office of Export Enforcement (OEE) agents to prioritized institutions and provides trainings of interest to academic institutions. This past July, we expanded the Initiative by adding nine more partner universities, for a current total of 29.

- 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 our 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 (VSDs). 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 Proposed Charging Letter – that Seagate continued selling millions of hard disk drives to entity-listed Huawei even after Seagate's only two competitors had stopped sales because of our Foreign Direct Product Rule (FDPR).

- 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. 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 year since the policy was announced, we have completed over 130 end-use checks in China.

- On April 18, 2023, I issued a second memorandum addressing our VSD policy, which also included policy clarifications regarding disclosures of potential misconduct by others. It has 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, Russian, Iranian, and other violators.

- On October 12, 2023, I publicly announced that we have changed the categories of what we measure internally to better reflect and further our prioritized enforcement efforts. More specifically, we have rethought our metrics – how we track our investigative and analytic efforts – so that we can best evaluate how close the fit is between our highest priorities and how we are spending most of our time. Starting with this new fiscal year, the annual performance plans for all of our managers now include a component on how well their field office's investigations, or leads generated by their analysts, connect to our highest-priority areas. With this enhanced focus, we will be able to better ensure that our finite resources are properly matched against the most pressing national security threats.

On the other major Export Enforcement program area, our antiboycott rules, I also have issued policy changes to enhance compliance, increase transparency, incentivize deterrence, and compel accountability for those who violate our nation's antiboycott regulations.

- On October 6, 2022, I issued a policy memorandum, and on October 7, 2022, we published regulations that re-ordered penalty tiers in the antiboycott regulations to better align categories of violations with our view of the violations' relative seriousness; raised penalty amounts to reflect our assessment of the seriousness of violations; eliminated "No Admit, No Deny" settlements; and announced an enhanced focus on foreign subsidiaries of U.S. companies to orient attention on the parties making antiboycott requests and not just the ones receiving them. Since these changes became effective, we have settled 4 cases resulting in penalties of $425,500, which is a significant increase in penalty amounts from previous years.

- On July 26, 2023, I issued a second policy memorandum further expanding and enhancing our antiboycott enforcement efforts in two ways. First, we amended the Boycott Reporting Form to include the name of the specific party making a boycott-related request to help the Office of Antiboycott Compliance investigate and hold accountable those making such requests. Second, in order to increase U.S. contractors' knowledge of and compliance with these rules, we worked with the Department of Commerce's Office of Acquisition Management to include a statement on the acquisition websites of both the Department and the U.S. Government (at www.SAM.gov) clearly articulating the requirements of the antiboycott regulations and their applicability to government contracts.

2. Technology Protection Partnerships

Second, given the scope of the threat that we face in protecting U.S. technology from misappropriation by nation-state actors of concern, we believe strongly in amplifying our efforts through robust partnerships – both domestically and internationally.

A. Domestic Partnerships

Domestically, we have developed partnerships with industry, academia, the Intelligence Community, Treasury components like the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN), DOJ, and sister federal law enforcement agencies like the FBI, Homeland Security Investigations (HSI), Customs and Border Protection (CBP), and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). These partnerships allow us in many instances to prevent diversions before they occur, and in others to impose costs on violators. Significant actions have included:

- Since its launch on March 2, 2022, we have been active participants in DOJ's Task Force KleptoCapture, an interagency effort aimed at enforcing the sweeping sanctions, export restrictions, and economic countermeasures that the United States has imposed, along with allies and partners, in response to Russia's illegal and unprovoked full-scale invasion of Ukraine.

- On June 28, 2022, we issued a joint alert with FinCEN establishing a new key term for financial institutions to reference when filing Suspicious Activity Reports (SARs) related to export evasion involving Russia. To date, we have reviewed over 500 filings, and we have been able to action nearly twenty percent of those SARs in various ways, including by cutting leads to our enforcement agents, advancing existing cases, and developing Entity List packages.

- In October 2022, we and DOD stood-up an interagency task force aimed at preventing and penalizing diversions of U.S. components found on the battlefield in Ukraine in Iranian unmanned aerial vehicle (UAV) systems. This same task force is now coordinating more broadly across the U.S. Government and with the Israeli Government to evaluate whether munitions being used by Hamas in or since its barbaric terror attack on Israel on October 7, 2023, contain any western components so that supply chain analysis can be conducted and future procurement efforts disrupted. We have a long history of working with DOD to counter Iranian procurements in support of its missile and UAV programs, including exploiting Iranian missiles and drones used by Houthis in Yemen against regional partners to identify diversion pathways. We have embedded an agent jointly with U.S. Central

Command and U.S. Special Operations Command to participate in DOD's Counter-Unmanned Aerial System (UAS) Working Group, which globally coordinates whole-of-government actions related to countering UAS programs of concern.

- On February 16, 2023, we announced the formation of the Disruptive Technology Strike Force in partnership with DOJ's National Security Division. 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 their military modernization efforts and 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 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 appropriate criminal and/or administrative enforcement action.

- On March 2, 2023, we issued a joint compliance note with DOJ and OFAC on the use of third-party intermediaries in transshipment locations to evade Russian- and Belarusian-related sanctions and export controls. The note informs the private sector about enforcement trends and provides guidance to the business community on compliance with U.S. sanctions and export laws.

- On May 19, 2023, we issued a supplemental alert with FinCEN regarding Russian evasion of U.S. export controls. The alert details evasion typologies, introduces nine new high priority Harmonized System (HS) codes to inform U.S. financial institutions' customer due diligence, and identifies additional transactional and behavioral red flags to assist in identifying suspicious transactions relating to possible export control evasion.

- On June 9, 2023, along with DOJ, Treasury, and the State Department, we issued guidance to industry on Iran's procurement, development, and proliferation of UAVs. The advisory highlights effective due diligence policies, compliance structures, and internal controls relevant to Iran's UAV-related activities to ensure compliance with applicable legal requirements across a company's entire supply chain.

- On July 26, 2023, we issued a second joint compliance note with DOJ and OFAC focusing on the voluntary self-disclosure policies that apply to U.S. sanctions, export controls, and other national security laws, including recent updates to certain of those policies, such as those in my April 18, 2023 and June 30, 2022 policy memoranda.

- On September 28, 2023, we issued "best practice" guidance encouraging industry to seek assurances of compliance from customers ordering the nine highest-priority HS codes sought by Russia for its missile and UAV programs, including through receipt of a signed certification statement. The guidance included a sample certification form to assist industry in implementing this best practice.

- On October 18, 2023, we, State, Treasury, and DOJ issued an advisory to industry alerting persons and businesses globally to Iran's ballistic missile procurement activities. This advisory provides information specifically relevant to the private industry in both the United States and abroad on the deceptive practices, key red flags, and other important indicators of ballistic missile-related procurement efforts by Iran.

- On November 6, 2023, we and FinCEN issued a joint notice establishing a new key term for financial institutions to reference in SARs related to export control evasion globally. This new key term enables us to receive SARs for potential export violations involving China, Iran, and illicit firearms trafficking, just like we do for Russia.

B. International Partnerships

Second, we 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 1,500 end-use checks in over 60 countries to prevent the transshipment and diversion of U.S. items in violation of our regulations, the highest number of end-use checks we have ever conducted. These checks were targeted directly at countering Russian and Iranian evasion through third countries, as well as monitoring exports directly or through third countries to China to prevent diversion to programs that could enable its military or human rights abuses. As noted previously, based on my October 7, 2022, policy memorandum aimed at addressing delays in the scheduling of end-use checks, we completed over 130 checks at Chinese companies in Fiscal Year 2023, an all-time high, eliminating a more than two-year backlog.

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 ECOs in Finland and Taiwan and an analyst in Canada, implementing a data sharing arrangement with the European Anti-Fraud Office (OLAF), and establishing export enforcement coordination mechanisms with export enforcement partners in Australia, Canada, New Zealand, and the United Kingdom (i.e., the "Export Five" or "E5") and G7 counterparts to prevent illicit reexports to Russia, Iran, and elsewhere, including China. Key efforts here involve exchanging information and best practices, as well as alerting industry of Russian evasion tactics. For example, in September, the E5 issued joint guidance for industry and academia addressing high priority items needed by Russia's military, explaining how exporters can identify Russian diversion pathways, and recommending due diligence that can be taken to harden supply chains.

With regard to our enforcement of controls on firearms, on November 17, 2022, we, ATF, HSI, CBP, Interpol, and the Caribbean Community (CARICOM) Implementation Agency for Crime and Security launched the CARICOM Crime Gun Intelligence Unit (CCGIU). The CCGIU provides intelligence analysis on illicitly trafficked firearms and ammunition and supports law enforcement agencies in Member States in the seizure of firearms, and related parts and components, as well as in identifying, charging, and prosecuting co-conspirators.

3. Enforcement Actions

Third, I want to highlight just some of the enforcement actions we have taken related to China, Russia, Iran, and illicit firearms traffickers so far in 2023.

- On January 17, 2023, Jonathan Yet Wing Soong pled guilty in connection with a scheme to secretly funnel sensitive aeronautics software to Beihang University, a university in Beijing that had been added to the Entity List due to its involvement in developing Chinese 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.

- On March 2, 2023, two Kansas men, Cyril Gregory Buyanovsky and Douglas Robertson, were arrested for an alleged years-long scheme that included the illegal export of aviation-related items to Russia after its full-scale invasion of Ukraine on February 24, 2022. Using KanRus Trading Company, the defendants allegedly conspired to evade U.S. export laws by concealing and misstating the true end users, value, and end destinations of their exports and by transshipping items through third countries to Russia.

- On March 9, 2023, a federal grand jury in the District of Columbia returned an indictment charging an Iranian national with the unlawful export of electrical cables and connectors from the United States to Iran. Mehdi Khoshghadam, Managing Director of Pardazan System Namad Arman (PASNA), an Iranian importer of electronics and other goods, allegedly used front companies located in China and Malaysia to make payments to a U.S. company for exports to Hong Kong that were then diverted to Iran.

- On April 20, 2023, we announced the largest standalone administrative penalty in BIS history – a $300 million penalty against Seagate for continuing to ship millions of hard disk drives to Huawei. When the Huawei FDPR went into effect, two out of the three major companies producing hard disk drives 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. The third company, Seagate, continued to sell and became Huawei's sole source provider for hard disk drives. This is the first enforcement case and penalty brought under the Huawei FDPR. 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.

- On May 11, 2023, DOJ announced the seizure of 13 domains used by Specially Designated Nationals (SDNs), including Specially Designated Global Terrorists (SDGTs), associated with Lebanese Hezbollah. A BIS Special Agent was the affiant on the warrant taking down these domains. This action directly impeded Hezbollah's ability to peddle its dangerous violent ideology across the globe.

- On May 16, 2023, DOJ announced the initial round of Disruptive Technology Strike Force cases with the filing of criminal charges by five different U.S. Attorney's offices in cases involving China, Russia, and Iran. In addition to the criminal charges, I issued a Temporary Denial Order (TDO) suspending the export privileges of five parties – Florida company MIC P&I, LLC, Russian airline Smartavia, freight forwarder Intermodal Maldives, and two of the charged defendants, Oleg Patsulya and Vasilii Besedin – for diverting civilian aircraft parts to Russia.

- On August 2, 2023, Robert Alcantara pled guilty to conspiracy to traffic firearms and conspiracy to launder money from his firearms trafficking, which carry sentences of a maximum of five years and 20 years in prison, respectively. ATF initiated the case against Alcantara, who purchased "ghost gun" kits and machined them into working firearms, which were then unlawfully exported to the Dominican Republic.

- On September 18, 2023, DOJ charged a Russian citizen residing in Hong Kong, Maxim Marchenko, with six counts related to the unlawful procurement of U.S. microelectronics with military applications on behalf of end users in Russia. Marchenko allegedly used shell companies based in Hong Kong and other deceptive means to conceal from U.S. Government agencies and U.S. distributors that the OLED micro-displays were destined for Russia. The items that Marchenko and his co-conspirators allegedly procured have significant military applications, such as in rifle scopes, night-vision googles, thermal optics, and other weapons systems. This case was coordinated through both Task Force KleptoCapture and the Disruptive Technology Strike Force.

- On October 31, 2023, three Russian citizens, Nikolay Goltsev, Salimdzhon Nasriddinov, and Kristina Puzyreva, were arrested on allegations they used two corporate entities registered in Brooklyn, New York to unlawfully source and purchase millions of dollars' worth of dual-use electronics on behalf of end users in Russia, including companies affiliated with the Russian military. Some of the electronic components and integrated circuits allegedly shipped by the defendants are the same make, model, and part number that have been found in seized Russian weapons platforms and signals intelligence equipment in Ukraine. Further, on November 7, 2023, we issued a TDO suspending the export privileges of seven persons and three companies alleged to be part of this illicit procurement ring. Both actions were coordinated through Task Force KleptoCapture and the Disruptive Technology Strike Force.

- On November 1, 2023, DOJ charged two Russian citizens, Nikita Arkhipov and Artem Oloviannikov, as well as Brooklyn resident Nikolay Grigorev, with an export control evasion scheme to benefit companies affiliated with the Russian military, including SMT-iLogic, a sanctioned Russian entity that has been identified as part of the supply chain for producing Russian military drones used in Russia's war against Ukraine. This case was coordinated through both Task Force KleptoCapture and the Disruptive Technology Strike Force.

In addition, we issued a record number of TDOs over the past fiscal year, demonstrating the power of our protective administrative measures to address violations of our rules. We issued or renewed 26 TDOs against Russian or Belarusian airlines for apparent violations of our expanded controls that were issued in response to Russia's full-scale invasion of Ukraine and nine TDOs involving Russian or Chinese parties to prevent imminent export violations. We also denied the export privileges of over 80 parties because they violated U.S. criminal laws prohibiting unlicensed firearms exports.

We 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 items subject to our regulations. While the Entity List is a licensing tool, the overwhelming majority of Entity List nominations come from the Export Enforcement intelligence analysts I oversee and frequently have ties to investigations conducted by our law enforcement agents. Currently, there are nearly 800 Chinese parties on the Entity List, of which over 300 have been added since the beginning of this Administration. Similarly, there are more than 900 Russian parties on the Entity List, of which over 600 have been added since the beginning of this Administration, as well as more than 200 parties in third countries tied to Russian evasion. We have also added more than 30 parties related to Iranian procurement in the past year, with a focus on Iran's UAV program.

As these cases and entity listings demonstrate, we leverage our administrative and criminal enforcement tools, as well as our regulatory authority, to address the diversion of advanced technologies – like semiconductors, marine engines, and satellite and rocket prototypes – to combat

the malign actions of China, Russia, and Iran, as well as to enforce our controls on the illegal export of firearms.

Conclusion

Thank you again for the opportunity to testify today about what we on the Export Enforcement side of the Department of Commerce's Bureau of Industry and Security are doing to help protect the national security of the United States. While export controls are only one set of tools in the U.S. Government's national security toolbox, the President's October 2022 National Security Strategy makes clear that export controls play a critical role in preventing our strategic competitors from exploiting foundational American and allied technologies, know-how, or data to undermine American and allied security. As the only agency in the U.S. Government whose sole mission is export enforcement, we remain laser-focused on enforcing our nation's dual-use export control rules.

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