UNITED STATES DEPARTMENT OF COMMERCE
Deputy Assistant Secretary for Export Enforcement
Washington, D.C. 20230

Statement of
Kevin J. Kurland
Deputy Assistant Secretary of Commerce for Export Enforcement
Before the Senate Homeland Security and Governmental Affairs Subcommittee on Emerging Threats and Spending Oversight
Hearing Entitled, "Improving Export Controls Enforcement"

April 10, 2024

Chair Hassan, Ranking Member Romney, distinguished Members of the Subcommittee, thank you for inviting me to testify on the Commerce Department's ongoing efforts to enforce U.S. export controls, including through interagency and law enforcement coordination efforts, and to help deny nation-state adversaries unauthorized access to U.S. technologies.

I currently serve as the Deputy 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 BIS with robust regulatory as well as administrative and criminal enforcement authorities that Export Enforcement leverages to protect U.S. national security.

At Export Enforcement, our talented law enforcement agents and analysts are focused on a singular mission: to keep our country's most sensitive technologies out of the world's most dangerous hands. Thanks to the authorities granted under ECRA, we have powerful tools to conduct this mission, which allow us to:

- inspect dual-use items anywhere in the United States;
- detain and even redeliver unauthorized shipments;
- conduct end-use checks overseas;
- issue administrative subpoenas;
- arrest suspects;
- work with our colleagues at the Department of Justice (DOJ) to bring criminal charges;
- impose stand-alone administrative penalties, including fines and denial of export privileges;
- inform the process of denying export license applications based on derogatory information derived from intelligence, enforcement, and other sources; and
- identify foreign parties for addition to the Entity List and Unverified List (UVL).

No other federal agency and, quite frankly, no other country, has so expansive a toolkit to enforce export control rules. Given the intentions and resources of our adversaries, our authorities, coupled with our partnerships with industry, other agencies – especially DOJ, the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the Intelligence Community (IC) – and international partners, have proven critical to protecting U.S. national security and foreign policy interests through aggressive enforcement of U.S. export controls.

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.

The 2024 IC Annual Threat Assessment identifies nation-state actors, especially China, Russia, Iran, and North Korea, as the most pressing threats, followed by transnational threats involving disruptive technologies that could lead to the rapid development of asymmetric threats. Accordingly, Export Enforcement's mission is laser-focused on preventing sensitive U.S. technologies and goods from being used for malign purposes by these nation-state actors and transnational threats. We do this in three primary ways: *prioritization* of our enforcement efforts on the most pressing threats; expansion of our *partnerships* at home and abroad; and aggressive *enforcement* of our controls.

Prioritization

First, we have prioritized our analytical and investigative work to match the evolving threat environment and the activities of malign nation-state actors.

We are focusing our attention on the technologies, end users, and end uses of most concern. This means targeting advanced technologies like artificial intelligence, supercomputers, quantum computing, electronics for use in military platforms like missiles and unmanned aerial vehicles (UAVs), and machine tools. It means focusing on the militaries, intelligence, and public security apparatus of our adversaries, as well as their defense contractors and other parties that enable their malign purposes, and transnational criminal organizations, such as those illicitly acquiring firearms and ammunition from the United States. And it means focusing on the misuse of items to support weapons of mass destruction, destabilizing military modernization, and the abuse of human rights.

When our analysts are reviewing license applications, targeting end-use checks abroad, and reviewing all sources of information for investigative leads and Entity List nominations, these three factors guide their efforts. Similarly, when our agents are conducting outreach to companies and academia to warn of diversion risks, detaining shipments, and investigating violations, they are guided by these three factors.

Our prioritized targeting of Chinese, Russian, and Iranian actors of highest concern also directly informs the identification of parties on the Entity List and targeting of end-use checks, which if they cannot be completed, can lead to additions to the UVL. Placement on the Entity List imposes a license requirement which effectively restricts the ability of parties involved in activities contrary to U.S. national security or foreign policy interests to obtain items subject to our regulations. The UVL identifies parties whose *bona fides* (i.e., their legitimacy and reliability) could not be verified during an end-use check and restricts the use of license exceptions as well as establishes enhanced recordkeeping requirements to prevent future diversions.

The overwhelming majority of Entity List nominations come from our Export Enforcement analysts 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 2020. Similarly, there are almost 1,000 Russian parties on the Entity List, of which over 660 have

been added since 2020, as well as almost 250 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. Combined, Entity List additions involving Chinese, Iranian, and Russian parties constituted approximately 80% of all listings in 2023.

In 2023, we 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. The overwhelming majority of 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 modernization efforts or human rights abuses.

As a result of these checks, we added 63 parties to the UVL in 2023, including 31 parties located in China for failure to schedule timely end-use checks. This action was the direct result of an October 7, 2022, policy memorandum issued by Assistant Secretary for Export Enforcement Matthew Axelrod aimed at addressing delays in the scheduling of 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 UVL. 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 has led directly to improved cooperation with our pending checks. Since the policy was announced, we have completed over 130 end-use checks in China and moved all Russian companies on the UVL to the Entity List.

Partnerships

Second, to expand the effectiveness of our robust enforcement authorities, we have partnered with industry and academia, other agencies, and likeminded countries to prevent diversion.

Industry, academia, and other relevant stakeholders – whether in the United States or abroad – represent the first line of defense in any effective export control system. We work closely with companies and universities to ensure they understand our rules and warn them of illicit procurement efforts, including through guidance on spotting red flags and implementing best practices to prevent diversion. We do this through our domestic outreach program and internationally through our Export Control Officer (ECO) program, where we have stationed now 11 officers in 9 locations worldwide,[1] along with an analyst in Canada.

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. We work daily with DOJ, FBI, Homeland Security Investigations (HSI), Customs and Border Protection (CBP), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the IC, and Department of the Treasury components like the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network. These

[1] ECO locations include: Beijing, China (2 ECOs); Dubai, United Arab Emirates; Frankfurt, Germany (2 ECOs); Helsinki, Finland; Hong Kong, China; Istanbul, Türkiye; New Delhi, India; Singapore; and Taipei, Taiwan.

partnerships allow us in many instances to prevent diversions before they occur, and in others to impose costs on violators.

Moreover, bringing together multiple agencies to address specific challenges has proven effective at leveraging complementary resources and authorities to achieve export enforcement objectives. These include:

- the Disruptive Technology Strike Force, which BIS and DOJ co-lead in partnership with FBI, the Defense Criminal Investigative Service (DCIS), and HSI to prevent nation-state actors from illicitly acquiring our most sensitive technology to advance their authoritarian regimes and facilitate human rights abuses;
- DOJ's Task Force KleptoCapture, which prioritizes BIS investigations involving Russian export control evasion for criminal prosecution;
- Project Cherry Bomb, which BIS co-leads with the Department of Defense to target Iranian UAV systems;
- DHS's Export Enforcement Coordination Center, where BIS holds a Deputy Director position to support the deconfliction of export enforcement cases across more than 20 federal agencies; and
- the FBI's National Counterintelligence Task Force as well as field office-level Counterintelligence Task Forces, where BIS participates as part of a whole-of-government effort to defeat hostile intelligence activities targeting the United States.

The Disruptive Technology Strike Force in particular gets at the heart of our prioritization strategy. The Strike Force focuses on preventing China, Russia, Iran, and other nation-state actors from acquiring disruptive technologies like quantum computing, artificial intelligence, and hypersonics that may eventually be powerful enough to deliver military overmatch, with the potential to alter the balance of power in the world. By bringing together experienced agents and prosecutors in 17 locations across the country, supported by an interagency analytical cell in Washington, D.C., we are able to use all tools in our collective toolboxes to address export violations. This includes sharing analytical and investigative resources across FBI, HSI, DCIS, and BIS, receiving prioritization, when appropriate, from DOJ on criminal prosecutions, and leveraging our unique administrative enforcement and regulatory authorities, including the imposition of Temporary Denial Orders (TDOs) and additions on the Entity List, to impose maximum pressure and consequences on procurement networks seeking to illicitly acquire disruptive technologies.

Additionally, we are working to build a constellation of enforcement coordination mechanisms with global partners. These include:

- establishing an analytical partnership with the Canada Border Services Agency through embedding an analyst in Ottawa;
- implementing a data sharing arrangement with the European Anti-Fraud Office (OLAF), which has access to customs data across all 27 European Union countries;
- launching the *CARICOM Crime Gun Intelligence Unit* with ATF, HSI, CBP, Interpol, and the Caribbean Community (CARICOM) Implementation Agency for Crime and Security to enforce firearms violations;

- establishing the "Export Five" or "E5" with Australia, Canada, New Zealand, and the United Kingdom and a Group of 7 working group on export control enforcement to exchange information and best practices on diversion networks, as well outreach to industry;[2] and
- organizing a Disruptive Technology Protection Network with Japan and South Korea that exports the Disruptive Technology Strike Force concept of operations to, and establishes interagency structures in, those two countries to enable joint investigative approaches and complementary enforcement outcomes.

Export Enforcement Operations

Third, we have 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.

Enforcement starts with encouraging industry to submit voluntary self-disclosures, as effective compliance is the first line of effective enforcement. Over the past year, we have updated our policies to further incentivize the submission of voluntary self-disclosures when industry or academia uncover significant possible violations of the Export Administration Regulations. This allows us to focus our efforts on the violations that can cause the most harm to U.S. national security. When companies disclose, they can receive penalty mitigation should we administratively charge them. Conversely, when companies do not disclose or simply flout our rules, we, along with our DOJ partners, will aggressively use criminal or administrative penalties, or both, to remedy the violative behavior.

I want to highlight some of the enforcement actions we have taken related to China, Russia, Iran, and illicit firearms traffickers since 2023 that demonstrate how we and DOJ, and many times through joint investigations with FBI, HSI, or other law enforcement partners, have addressed violations of our export control rules.

- 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 UAV 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 December 19, 2023, Buyanovsky, the owner and president of KanRus, pleaded guilty for his role in the scheme to circumvent U.S. export laws by filing false export forms with the U.S. government and, after

[2] 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.

Russian's full-scale invasion of Ukraine in February 2022, continuing to sell and export sophisticated and controlled avionics equipment to customers in Russia without the required licenses from the U.S. Department of Commerce. On March 19, 2024, Oleg Chistyakov, a Latvian broker who allegedly worked with Buyanovsky and Robertson to facilitate the sale of avionics equipment to Russian companies, was arrested in Latvia and remains detained pending extradition proceedings.

- 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 without a license. When the Huawei foreign direct product rule (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, BIS issued a 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 December 21, 2023, Alcantara was sentenced to 68 months in prison.
- 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 goggles, thermal optics, and other weapons systems. On February 29, 2024, Marchenko pleaded guilty to charges of money laundering

and smuggling military-grade technology to Russia. 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. On February 12, 2024, Kristina Puzyreva pleaded guilty to money laundering conspiracy for her role in the multi-million-dollar scheme to send components used in UAVs and guided missile systems to sanctioned entities in Russia. These 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.
- On December 6, 2023, DOJ charged a Belgian national, Hans Maria De Geetere, with crimes related to a years-long scheme to unlawfully export sensitive, military-grade technology, including accelerometers and missile components, to China and Russia. At the same time, De Geetere was arrested by Belgian authorities and he and his companies were added to the Entity List and to the Specially Designated Nationals and Blocked Persons List by OFAC. These actions were coordinated by the Disruptive Technology Strike Force.
- On January 17, 2024, Ilya Kahn, a citizen of the United States, Israel, and Russia, was arrested for his alleged involvement in a years-long scheme to secure and unlawfully export sensitive technology, including semiconductors, from the United States to Russia. As alleged, Kahn used a network of businesses in China and other countries to illegally transfer hundreds of thousands of semiconductors to a sanctioned business with ties to the Russian military and the Russia intelligence agencies. This case was coordinated through both Task Force KleptoCapture and the Disruptive Technology Strike Force.
- On January 31, 2024, Joly Germine of Croix-des-Bouquets, Haiti, the self-described "King" of a notoriously violent Haitian gang known as *400 Mawozo*, pleaded guilty to his role in a gunrunning conspiracy that smuggled firearms to Haiti in violation of U.S. export laws, and the laundering of ransoms paid for U.S. hostages to the gang in 2021. From at least January 12, 2020, 400 Mawozo was engaged in armed hostage takings of U.S. citizens in Haiti for ransom. The conspiracy resulted in the purchase in the United States of at least 24 firearms, including AK-47s, AR-15s, an M4 Carbine rifle, an M1A rifle, and a .50 caliber rifle, which were smuggled to the gang in Haiti.
- On February 5, 2024, Chenguang Gong of San Jose, California, was arrested for allegedly stealing trade secrets developed for use by the U.S. government to detect nuclear missile launches and track ballistic and hypersonic missiles. According to court documents, Gong transferred more than 3,600 files from the research and development company where he worked to personal storage devices, including blueprints for sophisticated infrared sensors

designed for use in space-based systems to detect nuclear missile launches and track ballistic and hypersonic missiles, and blueprints for sensors designed to enable U.S. military aircraft to detect incoming heat-seeking missiles and take countermeasures, including by jamming the missiles' infrared tracking ability. This case was coordinated through the Disruptive Technology Strike Force.

- On February 6, 2024, DOJ charged two Iranian nationals, Abolfazi Bazzazi and his son Mohammad Resa Bazzazi, with conspiring to export equipment used in the aerospace industry to end users in Iran. According to the indictment, the Bazzazis devised an intricate scheme to obtain commercial and military aircraft items from multiple U.S. companies for use in Iran's aerospace industry. This case was coordinated through the Disruptive Technology Strike Force.
- On February 12, 2024, DOJ completed enforcement of a final order for forfeiture of a U.S.-manufactured Boeing 747 cargo plane, previously owned by Mahan Air, a sanctioned Iranian airline affiliated with the Islamic Revolutionary Guard Corp-Qods Force (IRGC-QF), a designated foreign terrorist organization. Mahan Air, known to ferry weapons and fights for the IRGC-QF, violated export restrictions by selling the airplane to a Venezuelan cargo airline. The United States forfeiture of the Boeing 747 marks months of collaboration between the U.S. government and Argentine counterparts.
- On March 6, 2024, Linwei Ding was indicted with four counts of theft of trade secrets in connection with an alleged plan to steal proprietary information from Google LLC related to artificial intelligence technology. According to the indictment, Ding transferred sensitive Google trade secrets and other confidential information from Google's network to his personal account while secretly affiliating himself with PRC-based companies in the AI industry. This case was coordinated through the Disruptive Technology Strike Force.

In addition, we issued a record number of TDOs in the past 18 months, demonstrating the power of our protective administrative measures to address violations of our rules. We have issued or renewed 45 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 have denied the export privileges of over 125 parties because they violated U.S. criminal laws prohibiting unlicensed firearms exports.

As these cases and actions demonstrate, we leverage our administrative and criminal enforcement tools to address the diversion of advanced technologies – like advanced semiconductors, aerospace technologies, 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. As the senior career official in Export Enforcement, it is an honor and a privilege to work alongside such a talented cadre of agents and analysts that are focused on a single mission: to protect U.S. national security through the enforcement of our nation's dual-use export control rules.

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