Department of Justice

STATEMENT OF

EUN YOUNG CHOI
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE

EMERGING THREATS AND SPENDING OVERSIGHT SUBCOMMITTEE OF THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS

AT A HEARING ENTITLED

"IMPROVING EXPORT CONTROLS ENFORCEMENT"

PRESENTED

APRIL 10, 2024

STATEMENT OF
EUN YOUNG CHOI
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE
EMERGING THREATS AND SPENDING OVERSIGHT SUBCOMMITTEE OF THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

AT A HEARING ENTITLED
"IMPROVING EXPORT CONTROLS ENFORCEMENT"

PRESENTED
APRIL 10, 2024

Good afternoon, Chair Hassan, Ranking Member Romney, and distinguished Members of the Subcommittee, and thank you for the opportunity to testify on behalf of the Department of Justice. I am honored to be here representing the men and women of the National Security Division (NSD), who work every day to protect our national security with dedication, integrity, and professionalism.

NSD is charged with carrying out one of the Department of Justice's highest priorities: to defend the national security of the United States by pursuing justice under the law, including by investigating and prosecuting terrorism, espionage, sanctions and export control violations, foreign malign influence, and malicious cyber activity; overseeing and supporting the Intelligence Community's lawful use of surveillance authorities to acquire intelligence; and reviewing the national security risks of proposed foreign investments in U.S. companies. NSD regularly contributes to the whole-of-government response to the most serious threats we face as a nation.

I joined the Division in July 2023 as a Deputy Assistant Attorney General, and I oversee the Counterintelligence and Export Control Section (CES), the National Security Cyber Section (NatSec Cyber), and the Foreign Investment Review Section (FIRS). CES and NatSec Cyber are at the forefront of the Department's work enforcing our country's criminal laws related to cybersecurity, export control and sanctions, foreign malign influence, and espionage. FIRS leads the Department's efforts to protect national assets, such as sensitive data, communications, and technologies, by assessing, mitigating, and preventing national security and law enforcement risks before they materialize.

Today, the United States faces dynamic threats from a range of highly capable nation-state actors, including China, Russia, Iran, and North Korea. These nations engage in aggressive and sophisticated efforts, both inside our borders and abroad, to undermine the security, economic interests, and democratic institutions of the United States and our allies.

Nation-state adversaries seek to evade U.S. sanctions and export controls to develop capabilities that threaten international peace and stability. These countries work to obtain critical emerging technologies, including military hardware, cutting-edge semiconductors, and advanced computing capabilities. Such technologies pose significant dangers in the hands of our adversaries, with the potential to undermine advantages in U.S. and allied military capabilities. But the harms are not limited to military applications. Repressive regimes can use dual-use technologies like artificial intelligence, facial recognition, and advanced biotechnologies to conduct surveillance of civilian populations, stifle dissent, and enable human rights abuses.

Hostile nations are also accelerating their use of cyber-enabled means to carry out a range of activity targeting the U.S. government and American businesses and households. This includes stealing sensitive technologies, trade secrets, intellectual property, and personal data, as well as seeking access to hold our critical infrastructure networks at risk for destructive or disruptive attacks. While an increasing number of adversary nations conduct malicious activity in cyberspace, the People's Republic of China continues to stand apart in the breadth of persistent threats it poses to U.S. government and private-sector networks, including U.S. critical infrastructure.

As I discuss further below, a defining feature of NSD's work to combat these threats is our collaboration with interagency partners, including our work through the Disruptive Technology Strike Force.

I.

The mission and the changing threat landscape drive the National Security Division's enforcement priorities. The continued challenge posed by terrorism and the rising challenge posed by nation-state adversaries to the United States require even greater emphasis on the enforcement of the laws we use to defend against such threats.

Our adversaries are determined to unlawfully acquire advanced and sensitive technology from the United States and from our allies. For example, Russia is trying to circumvent heightened controls imposed on component parts being used in weapons systems against Ukraine. Because Russia needs this equipment to support its war effort and cannot manufacture enough of it domestically, it has turned to using third-party intermediaries and transshipment points to disguise the transfer of prohibited items and to hide the fact that the items are destined for Russian end users.

Countries like China, Russia, Iran, and North Korea have accelerated their use of cyber capabilities to carry out activities that threaten our national security, such as by stealing sensitive technology, intellectual property, and personally identifiable information; using online means to exert malign influences upon our democracy; generating revenue to evade sanctions regimes; and holding our critical infrastructure at risk of destructive or disruptive attacks.

To respond to these threats, the enforcement of U.S. sanctions and export control laws has been an increasingly vital tool in the fight to secure America's future against nation-state threat actors. NSD's CES is responsible for investigating and prosecuting criminal violations related to sanctions and export control laws and other related crimes.

Export controls are a critical tool to prevent our adversaries from eroding the technological advantage created by U.S. innovation and economic growth. The Commerce Department's Bureau of Industry and Security (BIS) and the State Department's Directorate of Defense Trade Controls (DDTC) are primarily responsible for regulating the export of commodities, software, technology, and services to other countries and foreign nationals, under the Export Control Reform Act and the Arms Export Control Act. BIS and DDTC use these authorities to prevent the export of sensitive items to our adversaries. NSD's CES prosecutes willful violations of U.S. export laws, working in concert with U.S. Attorneys' Offices and federal agents from BIS, the Federal Bureau of Investigation (FBI), Defense Criminal Investigative Service (DCIS), and Homeland Security Investigation (HSI). In certain cases, BIS, OFAC, and DDTC impose administration sanctions in conjunction with DOJ prosecutions.

In December, for instance, DOJ unsealed an indictment charging an Iranian national and his co-defendant, who worked for a Chinese company, with crimes related to the alleged procurement of U.S.-manufactured dual-use microelectronics for the Islamic Revolutionary Guard Corps (IRGC) Aerospace Force Self Sufficiency Jihad Organization's one-way attack unmanned aerial vehicle (UAV) program. In connection with that indictment, DOJ announced the seizure of more than $800,000 from companies tied to the procurement network.

Economic sanctions are a critical national security tool that seek to impose consequences on our adversaries and change their behavior by denying them access to the U.S. market and the economic benefits that come from doing business with the United States. Most economic sanctions programs are imposed by the President under the International Emergency Economic Powers Act (IEEPA) and administered by the Department of the Treasury's Office of Foreign Assets Control (OFAC). Sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to target countries and groups of individuals, including longstanding sanctions programs targeting Iran, Russia, and North Korea.

NSD's NatSec Cyber was announced in June 2023 to focus DOJ's efforts to counter nation-state, cyber-enabled threats to our national security. In particular, we have worked in close partnership with the private sector to disrupt infrastructure deployed by nation-state actors through technical operations, such as the court-authorized takedowns of the Cyclops Blink botnet and the Snake malware network, each of which were used to malicious ends by the Russian intelligence services, as well as the court-authorized takedown of the KV Botnet, which was used by Chinese state-sponsored actors to conceal their hacking of critical infrastructure.

NSD also works to disrupt other cyber-enabled activities that threaten our nation's security. For example, in October 2023, we announced a series of disruptive actions against a network of North Korean IT workers who, posing as Western computer programmers, used

online platforms to earn illegal revenue for North Korea's weapons programs from unsuspecting U.S. and other foreign companies. Through the seizure of fraudulent websites, asset freezes, threat intel sharing, and the related strengthening of anti-fraud measures, the U.S. government and private-sector partners disrupted this illicit revenue generation scheme, which implicated both cyber and sanctions authorities.

Economic espionage and the theft of trade secrets are also critical priorities for NSD. Our efforts are focused on combating our foreign state adversaries' efforts to steal cutting-edge and sensitive technologies and protecting companies where they are victims as well as prosecuting them when they facilitate such theft. In November 2022, for example, an intelligence officer for the Chinese government was sentenced to 20 years in prison for his role in a Chinese Ministry of State Security plot to steal commercial aviation trade secrets from U.S. companies to benefit Chinese state-owned aviation entities.

II.

The hallmark of our effort to respond to nation-state threats to our critical technology and economic security is interagency collaboration and partnership.

A critical example of this partnership is the Disruptive Technology Strike Force, which was created in February 2023 and is jointly led by the National Security Division and the Commerce Department's BIS. The Strike Force is an interagency enforcement effort designed to pursue criminal prosecutions and other types of enforcement actions against those who engage in the illicit transfer of emerging technologies in violation of U.S. laws.

The Strike Force consists of fifteen local cells across the country, which serve as enforcement teams made up of local federal prosecutors and agents from FBI, BIS, DHS's Homeland Security Investigations (HSI), and the Department of Defense's Defense Criminal Investigative Service (DCIS). In partnership with the National Security Division's CES, these local enforcement teams investigate and prosecute entities and individuals who violate U.S. laws governing the transfer of technology. The work of the local cells is supported by an interagency team of data analysts who coordinate case leads and identify opportunities to generate new leads.

The vision behind the Strike Force was to bring the collective resources of the U.S. government to bear to stop the flow of sensitive technology to our foreign adversaries. Each partner in this effort has an important role to play:

- BIS agents have authority under the Export Control Reform Act of 2018 to investigate export violations involving dual-use items and certain military items and present cases to DOJ for criminal prosecution, impose stand-alone administrative penalties, and add parties to the Entity List for acting contrary to U.S. national security or foreign policy interests.

- HSI agents are authorized to investigate violations of law involving military items, dual-use goods, and sanctions, with an additional focus on interdictions and other types of disruptions;

- The FBI, given its law enforcement and intelligence capabilities, is uniquely situated to investigate export violations with a nexus to foreign counterintelligence, and FBI's worldwide network of Legal Attachés provide valuable assistance coordinating with foreign law enforcement entities;

- DCIS, the criminal investigative arm of the DoD's Office of Inspector General, investigates the illegal proliferation and theft of critical DoD technologies and provides specialized expertise in the realm of procurement and supply chain fraud;

- DOJ, through its prosecutors in NSD and U.S. Attorneys' Offices, coordinates and partners with agents from each of these agencies to investigate violations of U.S. laws that protect sensitive technology. In many instances, prosecutors will work with multiple agencies to ensure that we deploy the full resources of the U.S. government.

Since its formation last year, the Strike Force has brought to bear the collective power of our resources against those who would seek to exploit technology to undermine our national security. In May 2023, we announced our first Strike Force cases, which were investigated and charged by five local cells from around the country alongside their CES partners:

- Two cases involved dismantling alleged procurement networks created to help the Russian government, including its military and intelligence services, to obtain sensitive technologies in violation of U.S. export laws. The technologies at issue include military tactical equipment, airplane braking technology, and quantum cryptography. In coordination with this action, BIS imposed Temporary Denial Orders against both procurement networks.

- Two additional cases charged former software engineers with allegedly stealing software and hardware source code from U.S. tech companies in order to market it to Chinese competitors. In one of the cases, the defendant was trying to sell the source code to Chinese state-owned enterprises. The stolen code is alleged to be trade secrets used by the U.S. companies to develop self-driving cars and advanced automated manufacturing equipment.

- The fifth case charges a Chinese national with violating U.S. sanctions in allegedly attempting to sell materials used to produce weapons of mass destruction to Iran. The defendant tried to arrange the sale using two Chinese companies that the U.S. government has sanctioned for supporting Iran's ballistic missile program.

Since that time, the Strike Force has announced nine additional cases, including charges against Russian nationals based in the United States and Canada who allegedly used corporate

entities registered in New York City to unlawfully source and purchase millions of dollars' worth of dual-use electronics on behalf of companies affiliated with the Russian military. The targeted technology included electronic components and integrated circuits with the same identifiers that have been found in Russian weapons and equipment seized in Ukraine. In March of this year, we announced the indictment and arrest of a Chinese national and former software engineer at Google for stealing from the company proprietary information related to artificial intelligence technology, a case that speaks to the Strike Force's continued focus on disrupting the evolving national security threats posed by AI and related technology.

Partnership and collaboration are also key components to the success of Task Force KleptoCapture, which the Department stood up following Russia's unprovoked and unjustified invasion of Ukraine in February 2022 and which is currently led by prosecutors from NSD and the Criminal Division. The goal of the Task Force is to ensure that oligarchs and other supporters of the Russian regime feel the full impact of the economic sanctions, export controls, and other economic countermeasures that the United States has levied in response to the Russian invasion.

Since its creation, the Task Force has focused on seizing and forfeiting assets and bringing prosecutions against those whose criminal acts enable the Russian government to continue its unjust war. Its successes include seizing, restraining, or obtaining forfeiture judgments against approximately $650 million belonging to Russian oligarchs and others who unlawfully supported the Russian regime and evaded U.S. economic countermeasures.

To date, the Task Force, in partnership with U.S. Attorneys' Offices and the National Security and Criminal Divisions, has charged more than 70 individuals and five corporate entities accused of sanctions evasion, export control violations, money laundering, and other crimes, many of whom have been arrested in more than a half dozen countries. Along with targeting the oligarchs and Russian elites who support Russia's unlawful invasion of Ukraine, the Task Force has been focused on investigating and prosecuting individuals and entities that leverage their skills and access to circumvent U.S. law for the benefit of sanctioned oligarchs and the Russian military. These facilitators include lawyers, money managers, as well as sophisticated procurement networks that supply the Russian military with continual access to Western goods. Notably, in February of this year, the Task Force charged and arrested two U.S. persons for allegedly engaging in a conspiracy to evade U.S. sanctions for the ultimate benefit of Andrey Kostin, the President and Chairman of Russia state-owned bank VTB.

Both Task Force KleptoCapture and the Disruptive Technology Strike Force illustrate the value of partnership. These efforts bring together federal prosecutors, agents, and analysts from multiple government agencies, with the participation of field offices across the country. This interagency collaboration enables us to coordinate lines of effort, develop case leads, and prioritize enforcement actions.

Along with interagency partnerships, we have been increasingly looking to leverage our international partnerships to enhance and strengthen our enforcement efforts, and our allies are

rising to the occasions. We have received assistance from our international partners, including Germany, Italy, France, Spain, Estonia, Latvia, Croatia, and Cyprus, to track down perpetrators and make arrests. And we have joined forces with our allies through work like the Russian Elites, Proxies, and Oligarchs (REPO) Task Force to ensure that our respective legal authorities are aligned and to share information to take concrete action, including imposing sanctions, freezing and seizing assets, and pursuing criminal prosecutions.

III.

As NSD's enforcement priorities have evolved to confront the current threats, our efforts increasingly interact with corporations and the business community. Responsible corporate actors are critical to protecting our national assets and are on the front lines of sanctions and export control compliance efforts. Their decisions about which entities to do business with—and which entities to avoid—can often be just as impactful as our law enforcement disruptions or actions, and their cooperation and earlier reporting can be critical to our ability to identify and punish violations.

The Department has changed its corporate enforcement policies to incentivize corporate responsibility and promote individual accountability—by clarifying and standardizing policies on voluntary self-disclosure and corporate cooperation and encouraging companies to retool their compensation systems, as needed, to promote compliance. The goal of the National Security Division's corporate enforcement program is to create the conditions for companies to invest in compliance programs that will prevent violations of our export control and sanctions laws, help them to detect violations that do occur, and report them to us.

We recognize that even the most well-designed and resourced compliance programs cannot prevent every violation of law, so when companies become aware that their employees may be committing crimes, we want the company to step up, report those facts to us, and help us to investigate and prosecute the individual offenders. To do that, NSD, like every Department component, has issued a policy that sets out how a company can obtain significantly more favorable treatment in a criminal investigation when it voluntarily self-discloses potentially criminal violations of our export control and sanctions laws. NSD's policy further sets forth guidance for when an acquiring company that makes a voluntary self-disclosure of criminal conduct by an acquired entity can qualify for protections pursuant to the Mergers and Acquisitions Policy.

NSD is also working with interagency partners at the Departments of Commerce, Treasury, State, and Homeland Security to issue multi-seal compliance notes to the private sector. These notes highlight enforcement trends, convey our collective expectations about compliance, and identify red flags and other signs of potentially illicit activity in financial and commercial networks. Since March 2023, we have issued advisories addressing the use of third-party intermediaries to evade Russia-related sanctions and export controls, recent changes to voluntary self-disclosure policies, Iranian procurement networks for UAV and ballistic missile technology, best practices for entities operating in the maritime and other transportation

industries, and compliance obligations of foreign-based persons with U.S. sanctions and export laws.

* * *

As we respond to dynamic and evolving threats to our nation's critical technology and economic security, we remain committed to using all legal authorities in our arsenal to defend against threats from state and non-state adversaries. Through our interagency and international partnerships, along with our collaboration with the private sector, we can safeguard our country's innovation economy and protect our nation's financial investments and development of technologies of the future.

I appreciate the opportunity to discuss these issues with you, and I would be pleased to answer your questions.