

IMPROVING EXPORT CONTROLS ENFORCEMENT

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

APRIL 10, 2024

Available via the World Wide Web: <http://www.govinfo.gov>

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



U.S. GOVERNMENT PUBLISHING OFFICE

55–522 PDF

WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	RAND PAUL, Kentucky
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	JAMES LANKFORD, Oklahoma
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
RICHARD BLUMENTHAL, Connecticut	JOSH HAWLEY, Missouri
LAPHONZA BUTLER, California	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Majority Staff Director*
WILLIAM E. HENDERSON III, *Minority Staff Director*
LAURA W. KILBRIDE, *Chief Clerk*
ASHLEY A. GONZALEZ, *Hearing Clerk*

SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

MAGGIE HASSAN, New Hampshire, <i>Chairman</i>	
KYRSTEN SINEMA, Arizona	MITT ROMNEY, Utah
JACKY ROSEN, Nevada	JAMES LANKFORD, Oklahoma
JON OSSOFF, Georgia	RICK SCOTT, Florida

JASON M. YANUSSI, *Majority Staff Director*
NICHOLAS F. CARON, *Policy Advisor*
SCOTT MACLEAN RICHARDSON, *Minority Staff Director*
MAGGIE FRANKEL, *Minority Professional Staff Member*
PAUL H.J. HURTON III, *Subcommittee Clerk*

CONTENTS

Opening statements:	Page
Senator Hassan	1
Senator Scott	10
Senator Romney	13
Senator Lankford	15
Senator Blumenthal	17
Senator Rosen	20
Prepared statements:	
Senator Hassan	31

WITNESS

WEDNESDAY, APRIL 10, 2024

Eun Young Choi, Deputy Assistant Attorney General, U.S. Department of Justice	2
Kevin J. Kurland, Deputy Assistant Secretary for Export Enforcement, Department of Commerce	4
James R. Mancuso, Assistant Director, Global Trade and Investigations Division, Homeland Security Investigations, Department of Homeland Security .	6

ALPHABETICAL LIST OF WITNESSES

Choi, Eun Young:	
Testimony	2
Prepared statement	33
Kurland, Kevin J.:	
Testimony	4
Prepared statement	42
Mancuso, James R.:	
Testimony	6
Prepared statement	50

APPENDIX

Response to post-hearing questions submitted for the Record	
Mr. Kurland	55

IMPROVING EXPORT CONTROLS ENFORCEMENT

WEDNESDAY, APRIL 10, 2024

U.S. SENATE,
SUBCOMMITTEE ON EMERGING THREATS AND
SPENDING OVERSIGHT,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 3:05 p.m., in room SD-342, Dirksen Senate Office Building, Hon. Margaret Hassan, presiding.

Present: Senators Hassan [presiding], Rosen, Blumenthal, Ossoff, Romney, Lankford, and Scott.

OPENING STATEMENT OF SENATOR HASSAN¹

Senator HASSAN. Good afternoon. This hearing will come to order. I want to welcome our very distinguished panel of witnesses, and thank you for appearing today to discuss what your agencies are doing to enforce export controls, and how Congress can enhance enforcement efforts to prevent our adversaries from illegally acquiring advanced technology.

I also want to thank Ranking Member Romney and his staff, and the ranking member will be here shortly. We are in the middle of votes, but I want to thank them for working with us on this hearing and the months of staff oversight that have led up to today. I appreciate our continued partnership to address emerging threats to our Nation.

To our witnesses, I look forward to hearing from each of you about trends in export control violations, your agency's unique role in enforcement, and how better agency coordination can help prevent our adversaries from accessing sensitive technologies. We look forward to hearing more about actions that Congress can take to prevent advanced technologies from flowing to bad actors while still working to maintain the United States' innovation edge and our place at the center of the world's economy.

By breaking our export control laws and acquiring sensitive U.S. technologies, our adversaries can grow their military and cyber capabilities. This represents a considerable threat to the United States' national security. This is why over the past few years, there have been significant efforts to improve U.S. export controls as au-

¹ The prepared statement of Senator Hassan appears in the Appendix on page 31.

thorities work to constrain efforts by countries like China to acquire sensitive dual-use technologies.

This focus is important, and I have been glad to see the administration consistently roll out updated guidance in export controls for emerging technologies. However, there is always more work to do. It is incumbent on Congress to ensure the effectiveness of actions taken by the Executive Branch, especially as it relates to inter-agency coordination.

I look forward to hearing from all of our witnesses about their efforts to enforce export controls and how Congress and the Federal Government can work together to keep the American people safe, secure, and free.

I will recognize Senator Romney in when he returns from voting for his opening statement. But what I thought I would do is get us started on testimony, and then when he comes, we can break for his opening statement. It is the practice of the Homeland Security and Governmental Affairs Committee (HSGAC) to swear in witnesses. If you will all please stand and raise your right hand.

Do you swear that the testimony you give before this Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Ms. CHOI. I do.

Mr. KURLAND. I do.

Mr. MANCUSO. I do.

Senator HASSAN. Thank you very much, and please be seated. Our first witness today is Eun Young Choi. Ms. Choi is the Deputy Assistant Attorney General (DAAG) in the National Security Division (NSD) at the Department of Justice (DOJ). Before overseeing export controls at the National Security Division, Ms. Choi was the inaugural director of the National Cryptocurrency Enforcement Team. In this role, she set strategic priorities to address crimes involving cryptocurrencies and digital assets.

Welcome, Ms. Choi, you are recognized for your opening statement.

TESTIMONY OF EUN YOUNG CHOI,¹ DEPUTY ASSISTANT ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Ms. CHOI. Good afternoon, Chair Hassan, and distinguished staff of the Subcommittee. I appreciate the opportunity to testify here today. I joined the National Security Division this past July after spending over a decade at the Department of Justice, eight years of which I spent as an Assistant United States Attorney (AUSA) for the Southern District of New York, focusing primarily on cyber investigations, including those implicating national security. Just before joining NSD, as you mentioned, I was the inaugural director of the National Cryptocurrency Enforcement Team, which focuses on the criminal use of digital assets.

The work of NSD is increasingly focused on responding to the evolving and dynamic threats posed by sophisticated nation-state actors such as China, Russia, Iran, and North Korea. These countries have sought to acquire sensitive technologies, including not only military hardware, but also emerging technologies such as ad-

¹ The prepared statement of Ms. Choi appears in the Appendix on page 33.

vanced computing and autonomous vehicle capabilities, as well as the components upon which these technologies are built, for instance, semiconductors and microelectronics.

Such technology in the hands of our adversaries, risk undermining us and allied military capabilities. It can also be exploited by repressive regimes to conduct surveillance of civilian populations suppressed descent, and enable human rights abuses.

Enforcing our export controls and sanctions laws is critically important to countering these threats to our natural security and requires interagency, international, and private sector cooperation. The Justice Department plays a central role in those efforts, investigating and prosecuting criminal violations of those laws alongside our law enforcement and interagency partners.

This interagency partnership is at the heart of the Disruptive Technology Strike Force (DTSF), which was established in February 2023, under the leadership of NSD in the Commerce Department's Bureau of Industry and Security (BIS), and is designed to pursue enforcement actions against those who engage in the illicit transfer of emerging technologies. The Strike force consists of 15 cells located across the country, made up of local Federal prosecutors and agents from four agencies, including the two represented here today, the Federal Bureau of Investigation (FBI) and the Defense Criminal Investigative Service (DCIS).

In close partnership with NSD's Counterintelligence and Export Control Section (CES), these local cells investigate and prosecute companies and individuals who violate U.S. laws governing the transfer of technology. Their work is supported by an inter-agency team of analysts who coordinate case leads and identify opportunities to generate new leads.

Since May 2023, the Strike Force has investigated and charged 16 cases across seven cells, and has secured guilty pleas from four defendants on exports, smuggling, and money laundering charges.

These cases include the arrest of a defendant who allegedly was engaged in a year's long scheme to illegally send sensitive technology, including semiconductors to a Russian entity with ties to the Russian military and the Federal Security Service (FSB), using a network of transshipment points in Hong Kong and other countries to try to evade tighter export controls put into place Following Russia's unlawful invasion of Ukraine.

The Strike Force also announced charges against four Chinese nationals who allegedly smuggled U.S.-origin items that could be used in the production of unmanned aerial vehicles (UAVs), ballistic missile systems, and other military-end uses through the use of front companies in China and Hong Kong for the benefit of the Iranian armed forces.

We recently marked the one-year anniversary of the Strike Force by bringing together the local cells to Phoenix, and holding a summit focused on case studies, best investigative practices, briefings on cutting edge technologies, and one-year reports of their efforts.

The work of the Strike Force builds upon the success of the Task Force KleptoCapture to capture, an inter-agency task force dedicated to enforcing sanctions, export and trade restrictions, that the United States has levied in response to the Russian invasion.

The task force's successes to date include seizing, restraining, or obtaining forfeiture judgments against almost \$700 million worth of assets belonging to Russian oligarchs and others who unlawfully supported the Russian regime and invaded U.S. economic countermeasures, and charging 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.

To that end, we have been leveraging our international partnerships to follow leads, track down perpetrators, and make arrests around the globe. Curtailing the flow of sensitive technology to our adversaries is a global problem and it demands a global response.

Finally, private sector partnership is critical to our work. Companies are on the front lines when it comes to export controls and sanctions. Their decisions as to how, where, and with whom to do business can be just as important as our criminal enforcement actions.

I appreciate the opportunity to discuss these issues with you and would be happy to answer any questions.

Senator HASSAN. Thank you very much for your testimony. Senator Romney, we just started testimony. We can go through with it or you can make your opening statement.

Senator ROMNEY. Oh, please continue.

Senator HASSAN. OK. Thank you. Our next witness is Kevin Kurland. Mr. Kurland is the Deputy Assistant Secretary for Export Enforcement at the Bureau of Industry and Security at the Department of Commerce.

He previously served as the Deputy Chief of Staff for the Undersecretary for the Bureau of Industry and Security. Before joining the Bureau of Industry and Security, he worked as an international trade analyst at a U.S.-based law firm.

Welcome, Mr. Kurland. You are recognized for your opening statement.

TESTIMONY KEVIN J. KURLAND,¹ DEPUTY ASSISTANT SECRETARY FOR EXPORT ENFORCEMENT, DEPARTMENT OF COMMERCE

Mr. KURLAND. Chair Hassan, Ranking Member Romney and distinguished Members of the Subcommittee. Thank you for inviting me to testify in the Commerce Department's ongoing efforts to enforce U.S. export controls.

I currently serve as the Deputy Assistant Secretary for Export Enforcement at the Commerce Department's Bureau of Industry and Security. 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 every day 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 identify, disrupt, and investigate any violations of

¹ The prepared statement of Mr. Kurland appears in the Appendix on page 42.

our controls. No Federal agency, and quite frankly, no other country has so expansive a toolkit to enforce export control rules.

At no point in history has export controls been more central to our national security than right now. The most recent annual threat assessment published by the intelligence community (IC) reaffirms that nation-state actors, especially China, Russia, Iran, and North Korea, are the most pressing threats. It also identifies transnational threats that can result from the misuse of disruptive technologies like artificial intelligence (AI).

Accordingly, Export Enforcement's mission is laser focused on preventing sensitive U.S. technologies from being used for malign purposes by these nation-state actors. 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.

My full testimony provides additional details on each of these lines of effort, but I would like to highlight a few key initiatives and actions that illustrate our effectiveness. First, we have prioritized our analytical and investigative work to match the evolving threat environment. We have updated our procedures for initiating enforcement leads and opening investigations to focus on the technologies, end users, and end uses of most concern.

We have been responsible for the addition of significant numbers of Chinese, Russian, and Iranian procurement-related parties to the Entity List, including ones announced just this morning. We conducted over 1,500 end use checks last year in over 60 countries, the highest number ever with the overwhelming majority targeting Chinese, Russian, and Iranian procurements, and transshipments of concern.

Second, to expand the effectiveness of our robust enforcement authorities, we have partnered with industry and academia, other agencies, including the intelligence community, and like-minded countries to prevent diversion. We work closely with companies and universities to ensure they understand our rules and to warn them of illicit procurement efforts.

We launched the Disruptive Technology Strike Force, which BIS and DOJ co-lead in partnership with Homeland Security Investigations (HSI), FBI, and DCIS to prevent nation-state actors from illicitly acquiring our most sensitive technologies to advance their authoritarian regimes and facilitate human rights abuses.

We established export enforcement coordination mechanisms with Canada, the European Union (EU), Five Eyes, and G7 counterparts, and we organized a Disruptive Technology Protection Network with Japan and South Korea to replicate the Disruptive Technology Strike Force model abroad.

Third, we have aggressively enforced our controls in a way that imposes real costs on those who seek to violate export controls and undermine U.S. national security. Our criminal enforcement efforts with DOJ last fiscal year (FY) resulted in the highest number of criminal convictions and number of months in prison on record.

On the administrative side, we resolved or imposed the highest number of administrative cases, denial orders, and temporary denial orders, including the largest stand-alone administrative penalty in BIS history; a \$300 million penalty against Seagate for con-

tinuing to ship millions of hard disc drives to Huawei, a party on our Entity List, without BIS authorization.

My testimony provides additional examples of high-profile cases dismantling illicit procurement networks involving China, Russia, and Iran, as well as of firearms traffickers.

Let me close by reaffirming that the work of our talented staff of 200 agents and analysts in partnership with industry, other agencies, and international counterparts has never been more important, and is achieving significant results that directly protect U.S. national security through aggressive enforcement of U.S. export controls.

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

Senator HASSAN. Thank you very much, Mr. Kurland. Our third witness is James Mancuso. Mr. Mancuso is the Assistant Director of the Homeland Security Investigations, Global Trade and Investigations Division, and Director of the National Intellectual Property Rights Coordination Center. Before his current role, Mr. Mancuso served as special agent in charge for HSI Baltimore. He also has served as the HSI attaché to the United Kingdom and Ireland.

Welcome, Mr. Mancuso. You are recognized for your opening statement.

**TESTIMONY OF JAMES R. MANCUSO,¹ ASSISTANT DIRECTOR,
GLOBAL TRADE AND INVESTIGATIONS DIVISION, HOME-
LAND SECURITY INVESTIGATIONS, DEPARTMENT OF HOME-
LAND SECURITY**

Mr. MANCUSO. Chair Hassan, Ranking Member Romney, and distinguished Members of the Subcommittee, thank you for the opportunity to appear before you today to discuss export enforcement, and the vital role Homeland Security Investigation plays as it stands at the forefront of U.S. counterproliferation investigations (CPI), and the enforcement of our nation's export statutes.

The enforcement of export control laws has been a critical element of U.S. national security dating back to 1789 when the first U.S. Congress and President George Washington created the United States Custom Service to interdict contraband under the United States, collect duties, and enforce our fledgling nation's trade laws. HSI formed under the Homeland Security Act of 2002 remains steadfast in its 234-year-old mission of enforcing our nation's export control laws.

HSI is a principal investigative component of the U.S. Department of Homeland Security (DHS), enforcing more than 400 Federal criminal statutes. The mission of HSI is to investigate, disrupt and dismantle transnational criminal organizations (TCOs) and national security threats seeking to exploit the customs and immigration laws of the United States.

HSI consists of more than 6,800 special agents assigned to 235 domestic field offices, 93 international offices in 56 countries. HSI is designated as the primary law enforcement agency charged with investigating violations of U.S. export laws related to military

¹ The prepared statement of Mr. Mancuso appears in the Appendix on page 50.

items, controlled dual-use goods, and sanctioned or embargoed countries.

I currently serve as the Assistant Director of the HSI Global Trade Division and the Director of the National Intellectual Property Rights Coordination (IPR) Center. The Global Trade Division provides oversight support for investigations of U.S. import and export laws to ensure national security, protect the public's health and safety, stop predatory and illegal trade practices, and prevent sensitive U.S. technologies and weapons from reaching transnational criminal organizations and foreign adversaries.

Global trade components include the Counterproliferation Investigations Unit, the Counterproliferation Mission Center, located in Huntsville, Alabama, and two whole-of-government centers; the IPR Center, and the Export Enforcement Coordination Center (E2C2).

HSI through its CPI program, brings to bear significant resources against sophisticated illicit procurement networks, which operate globally on behalf of transnational criminal organizations and other malign nation-states attempting to acquire U.S. military items and control dual-use goods. HSI's broad authorities combined with the extensive global footprint, has allowed its special agents to forge partnerships with domestic and international law enforcement communities. This is proving critical when illicit procurement networks exploit vulnerabilities in the global supply chain to circumvent laws for the purpose of illegally obtaining controlled goods and technologies.

Combating the illegal export and proliferation of sensitive technology equipment and weapons is an operational priority. Last year, the CPI program initiated over 1,500 investigations, made nearly 700 criminal arrests, worked with the Department of Justice to secure 371 indictments and 292 convictions, clearly demonstrating HSI unwavering commitment to national security.

The Export Enforcement Coordination Center was created in 2010 by Executive Order (EO) and serves as the primary forum within the Federal Government for executive departments and agencies to coordinate and enhance their export enforcement activities. HSI serves as the executive agency designated for the administration of E2C2, and is responsible to house, lead, manage, and fund the initiative.

The E2C2 two provides a whole-of-government approach to enforcement by ensuring inter-agency coordination, promoting multi-agency collaboration, and minimizing duplicative efforts and strengthening the critical link between law enforcement, the U.S. intelligence community, and export licensing entities. As a result of these partnerships, approximately 15,000 deconfliction requests have been processed by the E2C2 since becoming operational in 2012.

Export enforcement is critical to achieving our national security and foreign policy goals. HSI through its CPI program is uniquely positioned to effectively work with its partners in a unified effort to enforce our nation's export control laws.

I appreciate your interest in this important topic and look forward to your questions. Thank you.

Senator HASSAN. Thank you all three for your excellent testimony.

We are going to proceed to questions now, and I will start with a set of questions, and then turn it over to Senator Romney while I go vote.

To all three of our witnesses in your testimony, you each highlight the important and unique role that your agencies play in enforcing our export controls. Your agencies are working hard to protect our national security, but unfortunately, our adversaries are nimble, and they are constantly finding new ways to circumvent U.S. export controls.

Just this week, we saw concerning new reports that show how Iran is utilizing U.S. technology in weapons that it uses and exports to extremist groups and other hostile actors around the globe. I would like to hear about the new tactics that adversarial States like China, Russia, or Iran are using to avoid U.S. enforcement efforts and illegally obtain sensitive advanced technologies. Ms. Choi, we can start with you.

Ms. CHOI. I think it is important to recognize, and I appreciate that question, the interconnected nature of many of these adversaries. One way to think about it is for countries such as Russia and Iran, where U.S. economic countermeasures are quite comprehensive, they have incredibly robust procurement networks that involve shipment points in the use of front companies across the world, including in jurisdictions where it's sometimes difficult to hold people criminally accountable, such as, for instance, in our view China and Hong Kong, along with some of in the recent months since or in the recent years now, since the start of the unlawful invasion of Ukraine the countries that surround Russia, right?

I think one of the trends we are seeing is just how robust these procurement networks are, and we are doing the best that we can to try to find from the DOJ's perspective instances where we can identify willful participants in these procurement networks and holding them accountable to ensure that we can disrupt their ongoing flow of goods.

Senator HASSAN. Thank you. Mr. Kurland.

Mr. KURLAND. Madam Chair, what I would say is, we are focused on the activities of nation-state actors like China, Russia, Iran, and particularly their acquisition of advanced technologies, disruptive technologies, like AI, biotech, advanced computing, and quantum.

I think what is important to understand is these countries have both the intent and the resources to seek to acquire these items through any means necessary. That is what we are seeing on a day-to-day basis, whether it is licit acquisition, or illicit acquisition through cyber exfiltration, through theft, through the use of shell companies, through transshipments that is through shell companies.

This is a whole-of government-effort where they have resources, and maybe in the case of China, almost unlimited resources, to seek to acquire these goods. What we are doing as an interagency is, we are fighting back by basically leveraging the authorities and resources that we have across the interagency through this Disruptive Technology Strike Force model.

The idea is how do we get together Commerce, and HSI and FBI analysts, to identify how our adversaries are seeking to illicitly acquire those items, and then get prosecutors and investigators in cells all across the country to prioritize enforcement actions against those activities.

We have had a significant amount of success just in the first 15 months that the Strike Force has been in effect. Sixteen criminal cases have been brought. Just last month we had one involving a Google employee who was stealing AI software and technology to take it back to China. Their whole-of-government response requires us to be as similarly nimble and active to share our limited resources and our comprehensive authorities to go after those threats.

Senator HASSAN. Thank you for that. Mr. Mancuso.

Mr. MANCUSO. Much like my colleagues here at the table expressed, it is a whole-of-government approach, and that is one of the things at the E2C2 where we really rely on each other's unique authorities and, and different investigative methodologies and strategies to attack this problem set. I will go to a different direction and talk a little bit about partnership engagement with private industry. At the E2C2, we are regularly——

Senator HASSAN. I want to just stop you for a minute because what I was trying to get at was how China, Russia, and Iran are trying to avoid our enforcement effort. Then I want to move into the topic about kind of how we are responding to that.

Mr. MANCUSO. Sure. When we are talking about the relentless efforts of our adversaries, they are constantly attempting to acquire these components, this innovation, this creation, this technology, and it's important for the government to have that conversation with industry. No one knows their customer base like private industry.

When they are receiving a one-off request, when they are receiving something outside their normal supply chain and their red flags kind of go up, that is when we need to have an honest conversation with them. We have the ability, a two-way conversation, not just a one-way conversation with the government.

We start there, and then when we receive intelligence or referrals from our private industry partners that this may be a request from a bad actor, that is when law enforcement is involved. That is when we work with our industry partners and all the agencies, and then we do what we do best. We investigate that allegation.

Senator HASSAN. OK. Thank you. Mr. Mancuso. Another question for you, and then I will turn it over to Senator Romney. As you know, many of our foreign partners rely on their customs agencies to enforce export controls. Frequently, those customs agencies are not law enforcement agencies, and they may not have the authority to take direct action against criminals. As a result, there may be delays in turning intelligence into enforcement actions.

How does this situation impact Homeland Security Investigations' operations? How could Congress better enable HSI to act against international criminal organizations that break our export control laws?

Mr. MANCUSO. Thank you for that question. The subject of international overseas customs officers is very dear to me. I had the op-

portunity, the privilege, to serve as the attaché to the United Kingdom (UK) at the embassy in London for five years.

HSI has invested a tremendous amount of resources and efforts into a very healthy overseas footprint. And what it's allowed us to do is strategically align ourselves in different regions with our international partners to combat this.

Now, as legacy customs officers, I understand the challenges of working with our customs partners. One of the things I would say is we as HSI have looked at threats and we have been able to realign our resources to address today's threats. For example, we now have four HSI personnel in HSI Taipei. That was a strategic decision we made as an agency to counter the threat from China.

Conversely, in HSI Bucharest, we now have a presence there before the Russian invasion of Ukraine. They were working, spending an incredible amount of time, hand in hand with their Ukrainian customs counterparts recovering weapon systems from the battlefield, exploiting those weapon systems to see are there U.S. components in those, and if so, how do they get there? It is an incredible challenge.

Thank you for your interest in this. How could you help? I think one of the ways you could help would be ensuring that HSI in our FY 2025 budget, HSI is fully funded, therefore giving us the strategic ability to adjust resources internationally. The ability to turn on a dime and pivot, not just today's threats, but the threats tomorrow and five years down the road.

Thank you for just that topic.

Senator HASSAN. Thank you. I will return to this in another round of questioning with our other witnesses. Senator Romney.

Senator ROMNEY. I am going to yield to my colleague, Senator Scott, who has a hard stop on the other end.

OPENING STATEMENT OF SENATOR SCOTT

Senator SCOTT. I want to thank the Chair and Ranking Member, for hosting this hearing. Thanks each of you for being here. Thank you for what you do.

Mr. Kurland, I personally do not believe that the United States should be doing any business with Communist China Party (CCP). The CCP is not an honest trade partner. Just recently, we learned more details about American business executives being trapped in China with an exit ban just for civil litigation business disputes for as little as \$7,000.

They steal our intellectual property, use non-market economic practices to destroy our businesses, harness our technology and innovation for their military to defeat us, or to make the world dependent on Chinese-run technology. They cut corners at every turn, from the labor they use, to poisons they put in their foods that they normally export to America. Every U.S. dollar spent there supports the CCP's military and its horrific human rights violations based on the BIS count country report for China.

In 2022, only seven percent of export licenses for tangible items, technology, and software were denied. A whopping 3,249 were approved, and another 980 were returned without action. Approvals for licenses to export to China to remain at historically high levels.

Do you think this is an approval rating that we should be comfortable with?

Mr. KURLAND. Senator Scott, first of all, let me say that I share your concerns about China's illicit procurement of U.S. technology, particularly to support its destabilizing military modernization programs and mass surveillance programs.

I am on the export enforcement side of the house not the export administration side of the house that does the licensing. What I can tell you is, on our side, our team is focused on preventing and deterring China from illicitly acquiring technology to support these destabilizing programs. It is why we have stood up the Disruptive Technology Strike Force.

We have been using the administrative enforcement authority that we have under the Export Control Reform Act in an aggressive manner. We have imposed the highest stand-alone civil penalty in our history just this past year against a party that was selling hard disk drives to a party on our Entity List called Huawei a \$300 million penalty. We have imposed the most temporary denial orders in our history in just the past year.

In addition, we continue to aggressively use our Entity List to prevent China from getting access to key technologies. There are now over 800 companies, Chinese companies, that are already on the Entity List in addition to six that we are adding tomorrow. They were announced this morning, four of which are involved with providing AI chips to China's military modernization programs. They are going on the list tomorrow in addition to two additional Chinese parties along with United Arab Emirates (UAE) counterparts that were providing components to the Russian and Iranian UAV programs.

Last, I will say we have been working with our interagency colleagues and in particular Financial Crimes Enforcement Network (FinCEN) to receive from financial institutions suspicious activity reports that we can also action into enforcement leads with regard to China's evasion of our controls. We are systematically focused on preventing China from getting access to those technologies using all of the authorities that we have been authorized.

Senator SCOTT. If you look at the numbers, it seems like there is a basic presumption of approval rather than a denial. The denials is, it seems, like it is an anomaly. Do you believe that there should be reforms to the BIS review process so there is going to be better parameters in place to effective presumption of denial as opposed to the assembly baked in presumption of approval?

Look, and we also know the hardware's only as good as what it is running on it, but it seems BIS list is porous and clunky to deal with the panoply of threats that should be addressed for export limitations.

So No. 1 is, do you think we ought to have presumption of denial with anything with regard to China? No. 2 is, how do you consider software for inclusions on the list?

Mr. KURLAND. Senator every license application that goes through the Commerce system gets reviewed by the Department of Commerce, the Department of State, the Department of Energy (DOE), and the Department of Defense (DOD), and also gets intelligence information added to it. There is a fully informed decision

that is being made by an interagency body on each one of those activities.

Each one of those licenses are reviewed de novo, if you will, on their own merits based on review or a refresh of information that the Department of Commerce and our interagency colleagues have in terms of determining whether or not this is a reliable recipient of U.S. items. That is the basis on which those licenses are reviewed. In terms of software and—

Senator SCOTT. Still a pretty big number, right?

Mr. KURLAND. Certainly, Senator. There is a lot of trade between the United States and China, and so there is a lot of licenses that are received in the system, but it also shows that there is a lot of licenses that are subject to our control that are undergoing that four-agency scrutiny to determine whether or not there is a reliable recipient on the other end.

Senator SCOTT. What about software?

Mr. KURLAND. Certainly software in terms of its control is something that we control in addition to commodities and technology itself. It is intangible, but it also goes through that same licensing process. It does not matter whether it is internet protocol (IP), or software, or a widget that you can hold, all of those transactions go through our system through all four agencies in order to make a determination on whether to approve.

Senator SCOTT. Let us talk about TikTok. I saw a report this morning that that when you look at TikTok and compare it to Instagram, and you look at the messaging on Instagram versus TikTok, it is no if and buts about it, the Chinese government is targeting us. They are targeting our kids. They are targeting every citizen gets on there for the news. It is not a little bit biased. It is complete.

There is nothing on TikTok about Tiananmen Square. There is nothing on about Tibet, and it all supports pro Hamas, attacks Israel. I mean, it is complete. It is not a little bit, it is complete.

Knowing all that, do you believe that TikTok ought to be banned?

Mr. KURLAND. Senator, I am going to defer to my colleague from the Department of Justice on the topic of TikTok.

Senator SCOTT. OK.

Ms. CHOI. Senator, I think that the Department of Justice and its leadership would agree with your characterization of the national security threats that are posed by TikTok. It is our view that TikTok and its parent company ByteDance are presenting a clear and present danger to our national security. We are in support of the Foreign Adversary Controlled Application Bill because it covers both TikTok and any attendant or subsequent applications that may have similar concerns with regard to foreign adversary control over our data.

There are three different ways in which we think it's a concern for national security. First, in particular, TikTok, as you mentioned, collects vast amounts of personal data from more than 170 million Americans who actively use the platform. It also relies on a proprietary algorithm that was developed and maintained in China to determine what content to show, and what content not to show or to suppress to its users. Third, TikTok continues to rely

on PRC-based source code and employees to support its U.S. operations.

We think that the national security front in this regard is even more urgent because of the Chinese government's growing use and focus on its AI capabilities.

Senator SCOTT. All right. Thank you.

OPENING STATEMENT OF SENATOR ROMNEY

Senator ROMNEY [presiding.] Thank you, Senator Scott. I am going to ask some questions now, and then when the Chair returns, she will, I think, provide Senator Lankford the opportunity to speak, and then we will finally get to Senator Blumenthal.

A couple of questions. There is a great deal being written about the degree of leakage, if you will, of things that are not supposed to be exported from our country or from our friends that are somehow getting in the hands of adversaries of one kind or another. How great a part do you think that is? Is this a tiny share of those things that are most sensitive, or is this a pretty significant problem that that we need to address?

Any one of you can respond to that? Maybe I will go over to Mr. Mancuso, and I realize we have a lot of things in the list, and so some things they are not terribly interested in, but I am thinking particularly about large scale chips that go into or other key defense technologies. How much of that is getting through? Are we a sieve? Are we not really a sieve, but drip, drip, drip. What's the characterization of what's getting around our export controls?

Mr. MANCUSO. Thank you for that question. I can say this is the Assistant Director for Global Trade, I think the sheer volume of legitimate trade far outweighs the illicit trade that is going on. However, that small slice is of concern.

What you have is you have folks at this table, all the 20 partners at the E2C2, the intelligence community. All of us are completely laser-focused on retaining America's innovation, our creativity, our intellectual property, right? We developed the most advanced weapon systems of the world because of our ability to create this. We are the envy of the entire world. That also means our adversaries will stop at nothing to obtain this technology in these weapon systems.

With that being said, we are focused on this issue. We are an investigative agency looking at these agencies attempting to disrupt and dismantle the flow of this technology. It concerns all of us. Like I said, we are focused. I am also concerned the day that they do not want our technology, the day that we are not the world leader because that means that they have surpassed us and they have become superior. All of us at this table are laser-focused, making sure that date never happens.

Senator ROMNEY. Yes. I think there's a recognition that with regards to AI, in particular. It is very difficult to control the software. Some software on AI has already been put on open source and represents, in my view, a huge breach of poor judgment or breach of good judgment. It is poor judgment.

There are some who believe that the only way we are going to try and keep AI from being used in a most negative way is if we

limit the supply of the chips necessary to operate AI. Are we able to do that successfully, or is it like, no, we really cannot.

Mr. Kurland, do you have a sense of that?

Mr. KURLAND. At BIS, Senator, we have been imposing controls not only on entities that are involved in these types of diversionary attempts, but we have over the past year and a half rolled out a series of significant countrywide controls on China in addition to parties in not only that are resident there, but their actors that are sitting in third countries as well.

It is a complex problem set, and certainly with regards to the semiconductor ecosystem where the vast majority of chips are produced offshore, trying to identify potential violators is something that we all here are working hard to do using all source intelligence, putting together analytical cells that are trying to identify those activities, working hand in hand with industry to both prevent on the front side and then, if there are violations, imposing penalties that are high enough to deter others is critical. We have been doing that as an interagency. We have issued over a dozen multi-sealed documents just in the past year and a half that are trying to get at this problem set: how do we get industry to harden their supply chains and their distribution Networks.

Then, we are working globally, internationally. Chair Hassan mentioned some of the complications of our international partners in most of these jurisdictions. The licensing folks are actually disconnected from the enforcement folks, right, and that creates a bit of a gap because the enforcement folks do not know what's coming into the system that's being licensed, and the licensing folks do not actually know what's going out, which is the biggest vulnerability, the things that should be coming into the system that are not.

We have been working very closely. We have attachés similar to HSI that are stationed now in 10 countries around the globe, trying to get our international partners to increase their capacity to identify and then take enforcement action in coordination with us.

It's a challenge, but we are using all the tools at our disposal—industry, interagency, international—to try to get at making sure that these key technologies are not getting into those hands. Where we're identified it, we are either using criminal enforcement, administrative enforcement, or as I mentioned, just this morning, we added four companies to our Entity List in China that were explicitly diverting AI chips to the Chinese military weapons program so that we can alert industry and have them harden their supply chains when they are doing their due diligence of transactions.

Senator ROMNEY. What will the penalties be for those corporations that have been, if you will, shipping those chips into China?

Mr. KURLAND. Sure. They would be subject to criminal and/or administrative enforcement authority. Up to 20 years in jail, or \$1 million per fine. Then on the administrative side, we have a statutory maximum of \$365,000 or twice the value of each violation. And as in the case of Seagate that resulted in a \$300 million penalty to set a deterrence level to say we expect companies to put in place internal compliance programs when they are screening their transactions.

Then when they find a problem, they come to us voluntarily through what we call a voluntary self-disclosure to tell us because

if they do not do it, and there's a willful action where there's knowledge, then we are going to take aggressive action to try to deter others from violating and also putting those that are investing in compliance programs at a competitive disadvantage. We want to level that playing field at the same time.

Senator ROMNEY. Ms. Choi, who's been the most successful in being able to get the key technologies that are vital and we have endeavored to restrict? Is it China or is it Russia? We read stories about Russia being able to get technologies that they are using in Ukraine. At the same time, we read about China.

Just today, we have read more stories about China getting advantage of our technologies. Are they equally effective or is one more effective than the other?

Ms. CHOI. Senator Romney, I would say that—I would refer you to the annual threat assessment which focuses on China's efforts in particular. I would say both of those countries pose concerns, but with regard to China, that threat assessment notes that China seeks to become a world science and technology (S&T) superpower, and to use this technological superiority for economic, political, and military gain.

Among its various methods to do that, it includes means to acquire or steal IP, its cyber operations, and its illicit procurement. I would say China is laser-focused on trying to advance its science and technology program, and it's a focus for us at the Department of Justice.

Senator ROMNEY. Thank you. Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Senator Romney, thank you. Thanks all your work. This is a lot of behind the scenes, very technical, very legal work that makes an enormous difference for the country. I really do appreciate the ongoing work on this.

I have a question about Huawei. We have talked about for years in trying to be able to limit the proliferation of Huawei around the world and communication systems. Now in their partnerships for chips development and such, Huawei's become a hundred-billion-dollar company.

The question is, are we being effective in limiting them? Can we show real progress in future limitations for Huawei getting into our ally systems and into American systems? How do we actually show that as a metric for how we are protecting us, our technology, and our allies? Anyone can step in on that.

Mr. KURLAND. Senator, as you know, Huawei is a significant national security concern for us. They have been on our Entity List since 2019.

Senator LANKFORD. But they are still getting bigger.

Mr. KURLAND. Our Entity List is not necessarily aimed at preventing their growth, it's aimed at preventing them from misusing U.S. technology for their malign activities. I think we have a level of confidence that our entity listing, in addition to the use of the foreign direct product rule, has had a significant impact on their ability to leverage U.S. technology to conduct their activities.

Where we have had an opportunity to enforce our controls against Huawei, we have done it. I have mentioned the Seagate

case twice, but it's, I think, an example of how aggressively we are identifying violations. As it relates to Huawei, we have another case as well that we resolved back in 2021, I believe, involving Huawei. We are focused on preventing them from getting our tech.

Senator LANKFORD. OK, I get it. Again, and I do not want to be flippant to say your focus is to be able to stop them from growing. I understand they are a Chinese company. They are going to continue to grow. Our focus is trying to keep them out of the systems of our allies, and to keep them from stealing our tech and our technology as well in the process.

The concern all along has been the next Huawei, the other company that's coming up. Obviously, we have a lot of focus on Huawei at this point. Do we know at this point the next company that the Chinese are using to be able to basically do the exact same thing and to be able to go after technology? When you are doing the entities list, it is whack-a-mole all the time on it. How is that going as far as identifying those next companies?

Mr. KURLAND. What I can say, Senator, on that question is we are lashed up with the IC on a daily basis. We are reviewing information. We are evaluating trends that are happening in China, and we are amending our controls, when necessary, both in terms of countrywide and entity wide, or entity-specific, I should say, to address those concerns.

We have done that with regard to advanced computing, semiconductor manufacturing, a number of their key parties in terms of both equipment manufacturing and semiconductors themselves have been put on our Entity List. These actions do retard and delay their capabilities, but should we identify the next champion, certainly it is somebody we will actively review to determine whether or not they are involved in violation of our controls but also whether or not we need to take some other regulatory action against them to prevent their access to U.S. tech.

Senator LANKFORD. This is just a process question that is getting the information out to different companies to let them know, hey, this entity is now on our Entity List, because that's changing all the time. Have you been able to evaluate how quickly companies are able to get the information processed? Is there an expectation to say within the next 15 days, 30 days, or 90 days, that the changes are made in this? Because some of them may be in the middle of contracting in the process when they actually discover that. Walk me through the process of how that's actually distributed out to companies and how quickly that can turn around.

Mr. KURLAND. Sure. Senator, I will answer it two ways. One is from the government perspective, and then one is from the industry perspective. When we put parties on the Entity List, we are working hand in glove with U.S. Customs and Border Protection (CBP) and HSI to identify transactions the next day that would violate our regulations. Then we both have authority to detain those shipments, or if they are moving to have them redelivered. We have the ability to immediately take enforcement action against shipments that are moving in violations of our regulations.

In terms of industry, obviously, they are published in the Federal Register. But one of the things that we have made available is something called the Consolidated Screening List, which is a list of

all the proscribed parties that is updated in real time from Treasury, State, and Commerce that companies can simply just download into their IT systems.

There are commercial systems as well, but it's a free service that we offer where companies can just download that immediately upon—and they get notification. They can sign up through our website for notifications of updates. They can download it so that their screening system immediately picks up those changes.

Those are some of the ways that we are working—it's also a way for us to make sure that, in particular, small and medium sized enterprises, which may not have the resources to expend and buy commercial software for these entities, can simply just import that information for free into their IT system and have an automated way to screen their transactions

Senator LANKFORD. For enforcement itself, and you talked about that there are criminal penalties, obviously, for selling to those on the entities list. How quickly do you start enforcing those penalties? Because you may put on the entities list today, there's a contract that they actually do 3 weeks from now. Is that a criminal penalty that comes?

Again, not being flippant about it, trying to be able to find out how quickly we are able to actually move from, it's there to, we need to do enforcement to be able to stop and how quickly it moves to major fines versus this is a contact to you to say, stop, you may or may not have known.

Ms. CHOI. Senator Lankford, that's actually a very important part point. I would note that criminal enforcement is a very important part of the enforcement rubric. But with regard to penalties in particular, that does not happen until after we have adjudicated the criminal prosecution, right? We have to bring charges, there needs either to be a guilty plea or a trial, and then there has to be sentencing.

The penalties are oftentimes, somewhat distant from the original sort of understanding of the problem. But there are many non-criminal sort of circumstance or examples in which that information could be helpful. For instance, as Mr. Kurland was explaining, if there was new information that was available to a company that may prohibit them from entering into that transaction, that's still disrupting a potential opportunity for there to be an export violation because we are looking for opportunities short of criminal prosecution to stop and disrupt that threat.

Senator LANKFORD. Sure. Grateful to do that. Thank you. Thanks for the questioning time. I may follow up with you on some questions on university students that are foreign students here in the United States. That's a growing population. We are not going to try to cutoff all foreign students here, but there are challenges that are there when they are involved in research, and there may be the possible transfer of technology or information as well. I will try to follow up with some questions for that. Thank you.

Senator HASSAN [presiding.] Senator Blumenthal.

OPENING STATEMENT OF SENATOR BLUMENTHAL

Senator BLUMENTHAL. Thank you, Senator Hassan, and Senator Romney, for your leadership on this Subcommittee. As you may

know, I am Chair of the Permanent Subcommittee on Investigations (PSI). We are conducting an investigation into the flow of parts and components, semiconductors, chips, to Russia.

I recently visited Russia, as a matter of fact, with Senator Blumenthal. In the course of a meeting with President Zelinski, he handed me a folder with documents, photographs, charts, showing me how prevalent American chips and other components are in Russian weapons that they have recovered on the battlefield. Our own military and intelligence community confirms that the flow is prevalent and pervasive.

This issue is at one level, very complex and challenging. At the other level, it's very simple. This system is not working. This system is not working, and I want to know why. That's the purpose of the investigation we are conducting.

Our Subcommittee's inquiry shows added—reflecting significant jumps in the export of products from four of the largest United States manufacturing companies, Intel, Texas Instruments, AMD, and Analog Devices to five countries neighboring Russia, Kazakhstan, Armenia, Georgia, Finland, Turkey. In recent years, exports to these countries increased by huge orders of magnitude between 2021 and 2022. For example, we found exports to Kazakhstan rose by more than 1,000 percent, and they are continuing to rise.

Mr. Kurland, I am assuming that you are aware of these trends, the increased flow of United States technology to these countries, eventually becoming parts of Russian weapons used to kill Ukrainians. Correct?

Mr. KURLAND. That is correct, Senator.

Senator BLUMENTHAL. Have you asked the State Department or one of our agencies of government whether it's Treasury or some other country to bring increased pressure on these countries?

Mr. KURLAND. There is a whole-of-government effort, Senator, to bring pressure on these countries, particularly that are outside the coalition. We have a coalition of 39 countries that have agreed to impose substantially similar controls on Russia. The vast majority of these shipments that you are referencing are coming from countries that are outside of the coalition; countries like China, UAE.

Senator BLUMENTHAL. I mentioned five countries that do not include China or UAE. I mentioned countries like Finland and Turkey. Finland is part of North Atlantic Treaty Organization (NATO). Turkey is part of NATO. Other countries depend on us. I am assuming that more can be done. You mentioned in your testimony, Mr. Kurland that we have been providing "guidance" on spotting red flags and implementing best practices to prevent diversion to private industry.

What are those red flags and why aren't they working?

Mr. KURLAND. Sure. We have been working diligently with industry to provide them with as much information as we have about the evasion tactics of Russia. Some of those tactics are companies that did not exist prior to the invasion now exist and are receiving items that require some enhanced due diligence where they were receiving items unrelated from that.

Senator BLUMENTHAL. Let me just come right to the point.

Mr. KURLAND. Sure.

Senator BLUMENTHAL. Don't you agree that these American manufacturers have to know, looking at these trends, that something is awry here?

Mr. KURLAND. I think, Senator, that this is a complex supply chain, but industry needs to do more, and we are trying to do more. We are using our Entity List as aggressively as possible. I, personally, over the past few months, have signed out over 40 letters to the major distributors, manufacturers, and express carriers identifying—

Senator BLUMENTHAL. I have no question that you are doing your job, and you are doing it as well as you can, and you are doing it expertly and with consummate dedication. My question is, are the private companies reacting positively and promptly enough?

Mr. KURLAND. I think there is a general recognition that they need to do more. I share your concern that they need to do more—

Senator BLUMENTHAL. By general recognition, do you mean on their part or our part?

Mr. KURLAND. On their part. I have been personally talking with the major trade associations, with major companies. I know even our undersecretary has been reaching out. There's a recognition that these components are ending up in places that they shouldn't be.

We need industry to do a better job of hardening their supply chains, and we are making specific asks of them to try to do that. Taking a look at these lists of companies and stopping voluntarily to sell to them. Putting together more effective distributor relationships so that they can track who the actual end user of these components are. There's a lot that they can do that we are encouraging them to do.

Senator BLUMENTHAL. I apologize for interrupting, but as you know, my time is limited. When you say you are encouraging them, as the saying goes, talk is cheap. There's the blunt instrument of criminal prosecution, which is very difficult to do. People can say, oh, well, we ought to prosecute them. But obviously, there's mens rea and intent, and all the difficulties of doing an effective prosecution.

I was a prosecutor for quite a few years, not minimizing the difficulties, but there are not more effective instruments other than jawboning that can be brought to bear here on private industry or on the countries that are complicit because they are not completely immune to economic pressure and other kinds of pressure that has real world consequences in dollars, and cents, or otherwise?

Mr. KURLAND. We have increasingly been ratcheting up our controls. That is on the other side of the bureau, Senator. I am on the enforcement side of the house. I can speak specifically to how we are addressing the evasion of our controls as they relate to those that are in place, and that's why we are out talking with industry.

We are giving them as much guidance as possible. We are providing them with lists. But as our controls change we will effectively enforce those controls as well.

Senator BLUMENTHAL. My time has expired, but I would appreciate an opportunity to follow up with you on these issues. Again,

I appreciate the work that you are doing on this very difficult topic. Thank you. Thanks, Madam Chair.

Senator HASSAN. Thank you, Senator. Senator Rosen.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, Chair Hassan, and of course, Ranking Member Romney for your hard work on this really important Committee. Thank you to the witnesses for being here and testifying today.

I want to focus my questions on artificial intelligence, and of course, its potential role in aiding in our enforcement in this area, and so many others. Because one of the issues this Committee in particular has been focusing on is how government use of AI has the potential to dramatically improve how effective and efficient government is. Whether it's cutting waiting times for Americans seeking support from Federal agencies, Federal workers using data to root out fraud and focus their efforts on going after bad actors.

To all of the witnesses. How can data analytics and AI tools improve export control enforcement, and where are your agencies in the development and the adoption of these type of tools for this purpose?

We can start with you, Ms. Choi.

Ms. CHOI. Thank you for that question. The Department of Justice recognizes, as you do, Senator Rosen, that there's tremendous potential in the use of AI to improve the way in which we are defending our national security or protecting the American people. With regard to export controls in particular, I am sure that my colleagues at the table will be able to discuss more specifically the ways in which AI could be harnessed in the export control investigations portion of our type of our criminal prosecutions.

From the Department of Justice perspective, we are making sure that we are looking at AI as a tool, especially when it comes to litigation, to see if there are ways in which we can use it to generate leads, but also to do the data analytics that we need to when it comes to evidence, when it comes to documents, including in the export control realm, because of the tremendous amount of documents, for instance, that are in other languages. Unfortunately, I can only speak a few.

We want to make sure that prosecutors can understand and digest that evidence. I would note that you know, we are looking at also from the Emerging Technology Board and within the Department of Justice to ensure that we have safeguards so that we are using AI in this manner at the Department of Justice. That we can protect the rule of law and make sure that people's rights are not violated as a result.

Senator ROSEN. Thank you.

Mr. KURLAND. Senator, having access to AI is a critical function for us to do our job more efficiently and more effectively given the amount of data that we have available to us, whether it's classified, open-source.

Government data is vast. The ability for AI to be able to synthesize that information for an analyst at a terminal and to be able to use that to predicate a law enforcement lead that would result in an identification of a violation would be incredibly powerful.

I can say at the Department of Commerce, we do not have the resources at this point to be running AI in that manner. Currently we are running a pilot. But the money even that we are using for that pilot for AI is not in our base.

We have asked in our Fiscal Year 2025 budget for a \$3 million down payment to keep this pilot running. But, I think we are in agreement with the study from Centers for Strategic and International Studies (CSIS) that talked about the infrastructure backbone for BIS to have an infusion of resources that could upgrade our IT capabilities, particularly

Senator ROSEN. IT modernization?

Mr. KURLAND. Yes.

Senator ROSEN. Thank you. I have a few other questions I want to ask. Please, Mr. Mancuso.

Mr. MANCUSO. That's a great question. In terms of what we are doing with HSI and looking at our threats overseas, folks that are trying to go ahead and steal our technology and our creativity, we go through as HSI, some of our customs counterparts are international partners, a tremendous amount of trade data. Looking for those anomalies in the trade data.

Criminal networks are constantly shifting and adjusting their tactics to stay one step ahead. AI would potentially give us the ability to go through mass volumes of data and identify these one-off anomalies which could be an indication that there's a transshipment or an end user is going to repackage that and set it onto an adversary.

It's interesting. It's a topic that's top of mind. In the President's latest Executive Order, we were named, the IPR Center, our part for helping out industry on the electoral property side. What we did is we commissioned a study with Michigan State universities in anti-counterfeiting and product protection.

We are going to reach out to U.S. businesses and say two things. How can you harness the power of AI to protect your intellectual property, and what are the top threats to your organization from AI? These are things we are working on, I am excited to release.

Senator ROSEN. We will look forward to seeing that. But I want to talk in the time I have left about the dual-use technology investigations, because American firms, honestly, we are really at the forefront of the AI technology revolution. For the last few years, I led a Senate delegation to the Consumer Electronics Show in Las Vegas. Multiple companies unveiled to us their new semiconductor chips.

Last year, the Biden administration announced restrictions on the export of AI chips and manufacturing equipment to China in order to limit China's access to advanced semiconductors related to AI.

Mr. Mancuso, I will go to you. Given the rapid advancement in AI technology, the importance of the semiconductor chips in supporting the more powerful AI, these large language models, all this amount of data, what resources do you need to keep up with the expansion?

Mr. MANCUSO. Thank you for that question. There is no doubt that AI is evolving at a pace that's hard to keep up with. What we are doing at the E2C2 in this space is working with our partners

here at the table and the 20 other partners, and in terms of resources and commitment. Thank you very much for that.

Again, I would go back to the Fiscal Year 2025 budget and ensuring that HSI is funded to go ahead and give us the resources, and the flexibility to think strategically and to prepare for this, and to put resources in place to meet that challenge. Again, thank you for that, your leadership and interest in this topic.

Senator ROSEN. I am going to ask Mr. Kurland more broadly. What other dual-use technologies do you see as high risk? How should we help you as a Federal Government prioritize these technologies, because there are a lot out there? What do you need? How can we help?

Mr. KURLAND. Senator, thank you. We are really focused on the key disruptive technologies that have been identified by the intelligence community: AI, biotech, quantum, advanced compute.

From our perspective, we believe that if we have more resources—as we have been able to demonstrate under the Ukraine Supplemental—when we have more analysts, we are able to identify more violations of our controls. When we have more attachés overseas, we are able to conduct more end use checks that identify diversionary activities, and those predicate our law enforcement leads.

Senator ROSEN. We have to partner AI with the common sense of humans.

Mr. KURLAND. Yes, exactly.

Senator ROSEN. Yes, thank you.

Senator HASSAN. Thank you, Senator Rosen. I do have some more questions, so I appreciate the witness's patience this afternoon. I appreciate the questions that my colleagues have asked as well.

I want to go back to the question I left off on which was really about international cooperation. To Mr. Kurland and Mr. Mancuso, recent reporting noted that Russian manufacturers have been importing machine tools that are made in Taiwan, and then using those tools to produce weapons.

Taiwan is a strategic U.S. partner and should be working with U.S. authorities to counter Russia. How can we get Taiwan and other international partners to be more proactive in countering Russia. Mr. Kurland, we will start with you.

Mr. KURLAND. Madam Chair, I think it's important to start with that Taiwan is a member of the Global Export Control Coalition, which means it has committed to imposing complementary controls as 38 other countries have done. It is a critical player in the global semiconductor supply chain and other key technologies like machine tools.

Anybody that is a member of this coalition allows us to A, influence them because there is a need to harmonize controls, but also bring together our enforcement elements for cooperation and build their capacity. That's what we have been doing.

I actually came back last month from Taiwan speaking with officials: how can we help them build their capacity for enforcement and implementation. We have an export control officer that is stationed there funded on a 1-year Ukraine Supplemental. We have asked the Congress in FY 2025 to actually make that position per-

manent. But we have a person that's working every day with the Taiwanese authorities to get them to increase their capacity, and they actually have done that. In February, they amended their controls. They now have controls on 77 pieces of machine tools.

But that's the model that we are using with other close partners and allies. Which is, when you are part of the coalition, there's an expectation that you are going to keep pace with our changes in controls and that you are going to effectively enforce. We are working through our attachés overseas to help build that capacity.

Senator HASSAN. Thank you. Mr. Mancuso, anything to add to that question?

Mr. MANCUSO. I believe, it's a great question. Thank you. I believe earlier I discussed how HSI made a commitment to have HSI for HSI personnel stationed in Taipei. The mission there is to work alongside with their law enforcement, but it's also capacity building. It's also the greater partnership effort. It's sharing of best practices, and it's really being a good partner. That's what we are doing, HSI officers, agents overseas are doing. We are working hand in hand with our international partners. If it's important to them, it's important to us and vice versa.

It is establishing these critical relationships on a global basis so we can all rely on the global community to combat this threat. We cannot do this alone. The United States clearly, and our partnership at the table, we cannot accomplish this alone. You have to rely on your committed global partners and then demonstrating by investing with our agents there, we are demonstrating our commitment to them and this in time will breed success.

Senator HASSAN. Thank you. Now I want to turn to kind of a follow-up on what Senator Blumenthal was asking you about. Ms. Choi, so we know how important it is that the private sector research institutions in academia share information with law enforcement about our adversary's various attempts to break export control laws and illegally gain access to critical U.S. technology.

We understand how important it is that they share information with law enforcement and that private entities that engage in cutting edge research and development uphold the law, protect intellectual property. What is DOJ doing to coordinate with private entities to prevent violations of export control laws and stop adversaries from illegally accessing advanced technologies?

Ms. CHOI. Senator, I appreciate the question. The Department of Justice also believes that, companies are in the forefront of our efforts to protect national security in the ways that you have described. In a variety of different lines of effort, we have been engaging with companies in order to ensure that they are incentivized to come forward, be it through our voluntary self-disclosure policies, to notify the government when they see things that are happening within the confines of their business that would be of concern or potential criminal activity.

We also think it's very important to provide them with the actionable intelligence that they can use to strengthen their own compliance systems because I think prevention is always going to be a better solution, be it in the export control realm or in cyber, when it comes to trying to protect your intellectual property.

I know with regard to the export control, the Disruptive Technology Strike Force has been having a series of private sector engagements, including having fora in various large cities to try to bring industry that are in that area of jurisdiction to explain trends that are happening within that area and that industry.

But in addition, we are ensuring that we have compliance notes, which we had discussed earlier. Again, actionable intelligence that companies can use to arm themselves. The flip side of that is when companies are willing participants in criminal evasion of our sanctions and export control laws and other criminal violations. We are focused on increasing and making more robust our corporate enforcement regime as well.

Senator HASSAN. Thank you. I have a few more questions, but I wanted to turn to Senator Romney, if you have more questions.

Senator ROMNEY. Yes. I am going to ask an open-ended question which is what you would recommend that we do, if anything, to reduce the flow of technology from the United States, particularly that which has been limited by export controls, that nonetheless is finding its hands in Russia, China, and other places, in part, because it's so critical now with AI.

It has always been important, but now with AI, it's the national security implications of us not being able to manage the super semiconductors that are necessary for AI. It's really extraordinary. I wonder if I could offer suggestions. One is more coordination among different agencies in the United States whether we need to do a better job and establish some type of entity that does more coordination.

Another alternative, which is putting more burden on the shoulders of the of companies. Chip manufacturers, I mean Intel, AMD, and so forth, Analog Devices. Given the fact that we just heard from Senator Blumenthal that there was 1,000 percent increase in shipments to a neighbor of Russia of technology, which is ultimately clearly going to Russia.

There could be a requirement that on particularly highly sensitive items, not all the items that we put export controls on, but in certain highly sensitive items that a corporation must track where it's gone and where it is, and be able to provide that information to somebody to say, all right, yes, this is where it is. If they do not do that, that we fine them heavily or provide the sanctions.

I hate just finding more requirements for you guys and trying to say, well, we have to get more money to you, because we all know that dollars are hard to come by at the Federal Government level. How about, say, to corporations, if you are going to see a shipment something of high sensitivity to some nation that's not part of the coalition, then you have to track where it is and be able to report to us how much you have sent, to which company, and where those items have gone.

That means putting people in that country, tracking it, determining through an audit, whether I am looking for what are the solutions to this, because it is not working now. There's a great effort on our part, but they are finding ways around it.

So why don't we just go down the order that you each testified with any suggestions you have, as you know, very briefly, if you

know. If you were a king for a day, what should we be doing differently than we are doing, legislatively, or other ways?

Ms. CHOI. Senator, with regard to your specific thought regarding the burden or the changing standards as it applies to corporations. I will defer to Mr. Kurland on that. I know you said that you understand that resources are scarce. If I could just illustrate one example of the resources that are required to do these sophisticated cases.

In one sanctions case alone, I am thinking of there are multiple petabytes of data, which we had to analyze for one criminal case. We simply are at our wit's end when it comes to resourcing and doing the big data analytics, and we know our adversaries are doing with our data. We need to be able to do that and be armed to do that.

I would have that in mind when you are thinking about resourcing in the Fiscal Year 2025. One other thing that's maybe not so obvious, but is very important to us, is the reauthorization of Section 702. It's absolutely vital to all the national security work that we do, but in particular, I think it's important to highlight that in certain instances, we have been able to glean insights into the illicit transfer of technology and goods to hostile foreign state actors for the use of that particular tool.

We would be happy to give you more details in a classified setting, but that is incredibly vital to every single thing that we do day in, day out. Thank you.

Mr. KURLAND. Senator, I cannot respond to policy prescriptions. I am on the enforcement side. What I can commit to you is that if new actions are taken, we will commit to aggressively enforce those from our perspective that requires more analysts, more attaché overseas, more agents that are working with DOJ to bring criminal cases.

It gets back to that IT issue as well; better IT systems so that we can create efficiencies to identify these violators and then more quickly be able to bring those cases, whether it's a criminal case, whether it's an administrative case, whether it's an entity listing. We have the authorities. We have never worked better together as an interagency in terms of E2C2, Disruptive Technology Strike Force. We are working in a complementary manner and sharing those resources. But the more resources that we have, the more effective we can be.

Senator ROMNEY. Thank you.

Mr. MANCUSO. The important first step was, today, we are having a hearing highlighting the importance of this. No. 2, HIS, we are not a policy agency. We are not a regulatory agency. We are an investigative agency. As I have mentioned earlier, just ensuring that we have the resources to do what we do. We are, like I said, we have a very healthy global footprint, and we are working every day. The men and women of HSI are working with our international partners, and to continue that, I believe that again, is a recipe for success. Thank you.

Senator ROMNEY. Thank you. Madam Chair.

Senator HASSAN. Thank you very much, Senator Romney. I want to keep going at another aspect of this issue of how we work with private entities. As we have heard during this whole hearing, the

Export Enforcement Coordination Center does really important work coordinating interagency enforcement efforts and ensuring that information is shared among Federal agencies.

However, private entities don't have access to most US export data, making it more challenging for them to conduct due diligence and avoid working with bad actors who are trying to violate our export controls law. Is DHS considering ways in which it could share more data with U.S. companies with research institutions in academia to help them protect themselves against accidental violations of export controls.

Mr. MANCUSO. Thank you for that question. I think the answer is we are always evaluating what we are doing well against what we could be doing better. That's a question we ask ourselves every day, and we can never become complacent.

We do have an aggressive industry outreach. We do have Project Shield America where we are actively speaking to thousands of companies every year. We are going to research universities; we are talking to them. That is one thing we are doing. Could we do it better? I am sure we always could.

Senator HASSAN. Yes. Again, this is not a question about better. I share all of my colleagues' respect and real gratitude for the work that all of you and the people you work with do. What I am trying to get at is, do we have a way of sharing actual data that these entities could use, or is DHS exploring it?

Mr. MANCUSO. Sure. In certain circumstances, but we are limited. Some of the law enforcement sensitive data that we sit on, and there are limitations, what we can legally share with our partners too. We share with private to the greatest extent possible. That is part of a two-way conversation, but there are limitations on what we can share and how we can share it. We do to the greatest extent possible, but there are limitations.

Senator HASSAN. OK. Ms. Choi, the Disruptive Technology Strike Force, which was created last year, works across Federal agencies to coordinate with global partners and enforce export controls. As the Strike Force continues into its second year, how should it expand its collaboration with more of our partner nations?

Ms. CHOI. Chair Hassan, that's an excellent question. We are trying to increase our international cooperation in a variety of ways. As was previously mentioned, there's an effort underway pursuant to the Camp David meeting between the President and leaders from Japan and South Korea to ensure that we are well equipped to help strengthen those other countries' export control regimes as well. Because export control regimes, at least from a criminal perspective, it's very important for our authorities to be aligned and for the violations to be of the same kind in order for us to have a maximum impact for disruption.

We also have, as a matter of course, every criminal investigation that we have, we leverage the global footprint of both the Department of Justice and the international law enforcement agencies that we work with and their presence abroad in export control.

Senator HASSAN. OK. We heard earlier that just today, Commerce listed two UAE firms for supporting Russia and Iran's drone program. Is DOJ considering embedding personnel in hotspots for

export control evasion, like the UAE, and if so, does the Strike Force need additional resources or authorities to do that?

Ms. CHOI. Senator Hassan, I do not know about the specifics of the UAE information that you just outlined. I would say I am not aware of a particular effort from DOJ to enhance its UAE presence on export controls. I will say I am aware of many different engagements with UAE on a variety of different issues, including export controls.

Again, we can always do more with more. The extent that we would have further resources to allow for that travel and to build those partnerships, the muscle memory with our international partners, we would look forward to receiving that.

Senator HASSAN. OK, thank you. Mr. Kurland, earlier you mentioned that BIS would be adding six new entities to your agency list because they were providing AI tech to China. Can you tell the Subcommittee more about their efforts to undermine export controls? How egregious were the violations? What additional action should we be taking against those entities or individuals who are working for them?

Mr. KURLAND. Senator, there are four entities that will be listed tomorrow for seeking to acquire AI chips for China's military modernization program and military intelligence end users. Addressing China's whole-of-government approach to acquiring these advanced technologies is something that we are all focused on a day-to-day basis.

It requires significant resources and analyst overseas. You were just mentioning attachés that are overseas. We currently are located in 10 countries, including UAE and key transshipment countries like Hong Kong and Taiwan, to prevent those types of diversions, and then to help us identify enforcement outcomes when those are identified.

Senator HASSAN. OK. I want to follow up with you. Maybe we will learn more tomorrow, but what we are really trying to get at is a sense of what these entities are doing, because that helps obviously inform us about what the next steps are and how we can be helpful. I am, again, out of time. Do you have any more questions? All right.

I have one or two more, and I thank you guys again for your patience. Mr. Kurland, an end use check is when the Commerce Department physically inspects an export-controlled item in a foreign country to ensure that the item will not be used for illegal purposes after a request from the Commerce Department.

Foreign governments have 60 days to allow U.S. inspectors to conduct end use checks in their jurisdictions. If a foreign government does not allow end-use checks within that timeframe, the Commerce Department can take away export licenses. How does the Office of Export Enforcement (OEE) share data with law enforcement regarding countries that delay end-use checks? How does interagency data sharing help inform sector-specific enforcement and private industry engagement?

Mr. KURLAND. Sure. Thank you. You explained the program perfectly, Madam Chair, in terms of our law enforcement investigators doing these end-use checks.

First, let me say that the majority of our partners around the globe ask for a list of who we are going to do checks at, and many of them also participate on those checks. We currently have no issues with regard to conducting checks anywhere around the globe.

We had an issue back in October 2022 that resulted in a change of our regulations, which you were referencing, as well as a policy that Assistant Secretary Axelrod issued that said that if a host government, in that case it was China, did not schedule a check within 60 days because we had a backlog, we would put them on our unverified list.

Then our regulation change allowed us to move them to the Entity List, which basically imposes a license requirement on any item subject to our regulations if those delays continued. I am happy to report that based on that regulation change and the policy initiative, that it has spurred the government of China to eliminate the backlog and to continue to cooperate with us.

At this point you know, we are not having any issue globally with conducting checks, and we have tools in place to spur foreign governments that might attempt to delay completion of those checks.

Senator HASSAN. That's good to hear. We have had a very comprehensive discussion, and I am very grateful for the three of you for spending so much time and sharing your expertise with us. I want to thank you for joining us today, but I also always like to give witnesses a chance to highlight any aspect of your work, in this case, on export control enforcement that we did not cover.

If you feel like we have been comprehensive, you can say, "we are all set," but I just did not want to leave today without giving you each a brief chance just to touch on anything we have not gotten to today. I will start with you, Ms. Choi, and work right down the line.

Ms. CHOI. Thank you for that opportunity. I would just say that we remain very focused on export controls. I think we have covered a lot of topics today, and so I will probably cede the rest of my time. But certainly, I would just like to reemphasize that we appreciate your leadership, and yours Senator Romney and your focus on this particular issue.

Senator HASSAN. Thank you. Mr. Kurland.

Mr. KURLAND. Madam Chair, I would say that at Commerce, we continue to be singularly focused on protecting U.S. technology from being misappropriated by our adversaries.

To the extent that we have an ability to do more if the Congress is able to provide us with additional resources from our FY 2025 budget request, in addition to requests that have been identified by non-governmental organizations (NGO's), in terms of the Kiev School of Economics (KSE), AEI, CSIS. They all have identified you know, the fact that if we have more analysts, we have more export control officers overseas, we have more agents, we have better IT systems, we can be more even more effective as we are laser-focused on this problem set.

Senator HASSAN. Thank you. Mr. Mancuso.

Mr. MANCUSO. I just want to say on behalf of the men and women of HSI, especially the folks in the CPI realm, all of our men

and women at the E2C2, and in Huntsville, Alabama, thank you for the opportunity to appear before you today. You asked some great questions and we appreciate your time. Thank you.

Senator HASSAN. Thank you very much not only for your testimony today, but for everything you and the teams you work with the men and women in your agencies do to help secure our Nation. I look forward to continuing this conversation with my colleagues and constituents. I know you have given all of us a lot of ideas and identified some new problems for us to solve. We appreciate that.

The hearing record will remain open for 15 days until 5 p.m. on April 25th for submissions of statements and questions for the record. This hearing is adjourned.

[Whereupon, at 4:33 p.m., the hearing was adjourned.]

A P P E N D I X

Chair Maggie Hassan

Emerging Threats and Spending Oversight Subcommittee
Hearing on “Strengthening International Cooperation to Stop the Flow of Fentanyl into the United States”
March 20, 2024

OPENING STATEMENT

Good afternoon. Today’s hearing will focus on the steps that U.S. agencies and foreign countries need to take to stop the flow of fentanyl into the United States.

The vast majority of fentanyl and now other powerful synthetic opioids aren’t being produced in the United States; these drugs come from international drug cartels. And we know that these cartels have international supply chains, Mexican drug cartels, for instance, order precursor chemicals used to make fentanyl or other synthetic opioids from chemical manufacturers in China. Then the cartels synthesize the opioids in Mexico and smuggle the drugs across the southwest U.S. border. U.S. and international authorities must work together to dismantle these transnational criminal organizations and cut off their supplies, money, and illegal weapons.

Today’s hearing is an opportunity to look at the specific steps that Congress needs to take to disrupt the fentanyl supply chain and dismantle the deadly and violent criminal organizations that dominate the trade. And we need to develop these strategies with the understanding that the cartels are nimble – constantly shifting their methods to circumvent the law.

We also need to recognize that these cartels take advantage of our current crisis at the Southern Border – so we need, urgently, to strengthen our defenses there. We should provide more resources to border agencies, hire more personnel, and deploy more equipment that can detect drugs in all kinds of vehicles.

However, as I noted, to have a lasting impact on the flow of fentanyl into our country, we need to work with our international partners to fully dismantle the drug cartels producing and supplying the drugs. When I participated in a bipartisan congressional delegation to China last fall, I pressed President Xi to do more to stop the manufacturing and exportation of fentanyl precursor chemicals. President Biden held a summit with President Xi a month later, and since then the Chinese government has said that it would do more to crack down on drug trafficking and target the profits of illegal drug and precursor chemical exports.

We have to hold China accountable and push them to implement reasonable, common-sense controls to limit illegal chemical exports. Yet China continues to resist calls to implement “Know Your Customer” protocols for its chemical sector. These protocols would require that companies verify that their customers have a legitimate purpose for dual-use chemicals and would make it much more difficult for drug cartels to purchase the chemicals that they need to make fentanyl. We must exert more diplomatic pressure to get this done, including working with other major Chinese trading partners to force changes.

U.S. agencies should also take steps to improve coordination and information sharing with Mexican authorities. The drug cartels operating in Mexico are extremely powerful. Their dangerous influence has corrupted officials at all levels of government. In the face of these challenges, we have to find reliable partners to dismantle the drug cartels.

One of the ways to dismantle and defeat the cartels is by depriving them of the money and illegal weapons that they smuggle across the southern border from the United States, something that Mexican officials have stressed to me in my two Congressional trips there. Cartels use these weapons and money to seize control of Mexican communities and bribe or kill officials. That is why I have worked with Senator Lankford to introduce the Enhancing Southbound Inspections to Combat Cartels Act. This bill requires that the Department of Homeland Security increase its inspections of vehicles and pedestrians traveling into Mexico. These inspections will help us prevent the flow of illicit money and weapons. The bill also authorizes additional resources for the border and law enforcement agencies that are responsible for inspections and investigations. I hope that the Senate Homeland Security and Governmental Affairs Committee will consider this legislation soon.

No one law alone will address the fentanyl crisis. Fentanyl is inexpensive to make and transport, and it is in high demand. It will continue to take an all-hands-on-deck approach to dismantle the cartels, crack down on the spread of illicit fentanyl, and protect our communities. That's why while we work to combat the cartels, we should also take steps to strengthen resources for people dealing with addiction to make sure that anyone who needs treatment and recovery services can access them.

Today, though, I look forward to discussing how we can disrupt fentanyl supplies and dismantle drug cartels with our three insightful witnesses. People in every corner of the country – including my home state of New Hampshire – have had their families and communities destroyed by the fentanyl crisis. We must do everything that we can to dismantle and defeat the cartels. We cannot relent in our efforts to build a safer future for our country and our children.



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

SENSITIVE BUT UNCLASSIFIED

**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.

SENSITIVE BUT UNCLASSIFIED

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.



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.



U.S. Immigration and Customs Enforcement

STATEMENT

OF

JAMES R. MANCUSO
ASSISTANT DIRECTOR
HOMELAND SECURITY INVESTIGATIONS

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
DEPARTMENT OF HOMELAND SECURITY

REGARDING A HEARING ON

"Improving Export Controls Enforcement"

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS
SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

April 10, 2024
342 Dirksen Senate Office Building
3:00 PM

Chair Hassan, Ranking Member Romney, and distinguished members of the Subcommittee on Emerging Threats and Spending Oversight.

HSI Counter-Proliferation Program

Export enforcement is more important than ever as we see our adversaries' persistent appetite for U.S. technology. An analysis of Russian military equipment in Ukraine showed how dependent the Russians are on Western manufacturing, in particular U.S. technology.¹ However, Russia is not the only nation integrating U.S. technology into military weapons systems. In August of 2022, Russian forces in Ukraine were utilizing Iranian-made Shahed-131 and Shahed-136 drones.² Some of the drones' microchips and global positioning components were of U.S. origin.³ Homeland Security Investigations (HSI) has been proactively investigating these misuses of U.S. technologies, which further illuminates the importance of export enforcement.

The HSI Counter-Proliferation Investigations (CPI) program was designed to protect the integrity of the U.S. export control system; prevent the unlawful export of sensitive U.S. commodities software, technology and services; and counter the threats posed by foreign adversaries, terrorist, and criminal networks seeking to acquire such items. HSI addresses these export concerns in a three-pronged approach: interdiction, investigations, and international cooperation. Furthermore, the HSI authority and experience in export enforcement originates with our predecessor agency, the U.S. Customs Service, preceding the creation of the Department of Homeland Security. HSI Special Agents still retain that same Customs authority. This unique authority allows HSI the flexibility to target illicit networks that utilize the global trade system to procure sensitive U.S. technology. The smuggler's method and diversion routes are not unique to any merchandise being illegally exported. The Customs Service recognized the importance of industry support and, in 1983, established its first public awareness program on export control, Project Gemini. HSI addresses trade system vulnerabilities as an agency by utilizing all the investigative disciplines within its portfolio.⁴ HSI continues to promote public awareness through a successor outreach program, Project Shield America. The Project Shield America presentations are designed to alert businesses within the export industry that their commodities, technology, or information may be destined for an inappropriate end-use, end-user, or destination.

HSI's CPI program is divided into three units: the Counter-Proliferations Investigations Unit; the Counterproliferation Mission Center (CPMC), formerly Exodus Command South; and the Export Enforcement Coordination Center (E2C2). Each unit focuses on specific export programs while working together to address broader export enforcement issues. The E2C2 was established by Executive Order 13558 under President Barack Obama. The E2C2 promotes a whole-of-government approach to export enforcement by ensuring interagency coordination and interagency

¹ James Byrne et al., *The Orlan Complex: Tracking the Supply Chains of Russia's Most Successful UAV*, (London, United Kingdom: Royal United Services Institute, December 2022), 9-10, <https://static.rusi.org/SR-Orlan-complex-web-final.pdf>.

² Knights, Michael and Alex Almeida, "What Iran's Drones in Ukraine Mean for the Future of War," The Washington Institute for Near East Policy, November 10, 2022, <https://www.washingtoninstitute.org/policy-analysis/what-irans-drones-ukraine-mean-future-war>.

³ "Explainer: American Parts in Iranian Drones," United States Institute of Peace, March 1, 2023, <https://iranprimer.usip.org/blog/2023/mar/01/explainer-american-parts-iranian-drones>.

⁴ *Seizure of Iraqi Assets: Testimony before the Subcommittee on Commerce, Consumer Protection, and Competitiveness*, 102nd Cong 4 (1991) (statement of John C. Kelley, Jr., U.S. Customs Strategic Investigations Director).

collaboration, minimizing duplication of efforts, and strengthening the link between law enforcement, U.S. intelligence, and export licensing entities. The E2C2 is led by an HSI director, with deputies from the Departments of Commerce and Justice..⁵

The People's Republic of China

The People's Republic of China (PRC) is the only near-peer with highly advanced military and technological power to compete with the United States. As stated in the National Counter-Intelligence Strategy for 2020-2022, the PRC operates worldwide using all instruments of national power to target the United States..⁶ The Chinese Government, Chinese-based transnational criminal organizations, and non-traditional Chinese operatives routinely violate customs and immigration laws enforced by HSI. These activities subvert U.S. laws in pursuit of the PRC's own national, economic, and military interests and jeopardize U.S. national and financial security.

For example, China has implemented policies which encourage or require the transfer of American technology and intellectual property to entities in China. These actions may hinder U.S. exports, deprive U.S. citizens of fair remuneration for their innovations, divert American jobs to the PRC, and otherwise undermine American manufacturing and innovation..⁷

To enhance the HSI efforts to counter these persistent and evolving threats, HSI launched Operation Red Umbrella in October of 2020, a multi-pronged strategic action plan designed to combat PRC related criminal activity. Operation Red Umbrella's strategy rests upon a whole-of-agency approach to enhance efforts to counter China across various HSI programmatic disciplines. The strategy advocates a cooperative enforcement approach to identify and dismantle PRC related criminal organizations violating U.S. laws and uphold U.S. security and public safety interests. HSI also seeks to prevent the exploitation of sensitive research, the probing of critical infrastructure, and the coordinated efforts of the PRC related to illicit Chinese finance activity, transnational repression, fentanyl smuggling, human trafficking, and a myriad of other related threats. Due to PRC-related efforts, HSI initiated 32 percent more export and sanction cases in Fiscal Year (FY) 2023 than in FY 2022.

Russian Federation

Russia has repeatedly employed unfair and illegal methods to acquire commodities and technologies needed to advance its national objectives. Russia is increasing its non-conventional military capabilities through emerging and disruptive technologies, including artificial intelligence, space capabilities, hypersonic weapons, quantum information science, and biotechnology. Beyond strengthening itself, Russia may also facilitate illicit proliferation to amplify instability around the world.

⁵ Exec. Order No. 13558, 3 C.F.R. 69573 (2010), <https://www.govinfo.gov/content/pkg/FR-2010-11-15/pdf/2010-28854.pdf>.

⁶ National Counterintelligence and Security Center, *National Counterintelligence of the United States of American for 2020-2022* (Washington, DC: Office of the Director of National Intelligence, 2020), 2 https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.

⁷ U.S. President, Memorandum, "Addressing China's Laws, Policies, Practices, and Actions Related to Intellectual Property, Innovation, and Technology, Memorandum of August 14, 2017," *Federal Register* 82, no. 158 (August 17, 2017): 39007, <https://www.federalregister.gov/documents/2017/08/17/2017-17528/addressing-chinas-laws-policies-practices-and-actions-related-to-intellectual-property-innovation>.

After the Russian invasion of Ukraine, HSI coordinated an agency-wide effort focused on Russian state-owned industries, financial institutions, government officials, and oligarchs who flagrantly disregarded U.S. export controls and economic sanctions. Furthermore, in support of the Department of Justice's Kleptocapture Task Force, HSI worked to identify, locate, and bring to justice those individuals who were enabling the Russian regime to continue its unprovoked invasion of Ukraine. HSI will continue to use its civil and criminal asset forfeiture authorities to seize and forfeit assets linked to sanctioned individuals and/or proceeds of unlawful conduct that empower the Russian Government to continue the Russia-Ukraine war.

Additionally, HSI is leveraging Ukraine battlefield exploitation to identify U.S. components used within Russian weapon systems and target those procurement networks engaged in resupply efforts. With the data from these efforts, HSI develops leads for its domestic and international offices to target the proliferation networks, brokers, end-users, finances, and front companies that Russia uses to subvert U.S. and Western export controls and sanctions. Russian efforts to procure U.S. technology has led to an 85 percent increase in HSI case initiations on Russian tied export and sanction investigations from FY 2022 to FY 2023.

Lastly, to ensure deconfliction and coordination, E2C2 leads an interagency working group that shares information on Russian diversion efforts. The team comprises personnel from the Department of Commerce's Bureau of Industry and Security, HSI Counterproliferation Mission Center, U.S. Customs and Border Protection, and Department of Energy. The working group analyzes U.S. export and open-source trade data to identify trends indicating possible diversion of U.S. goods.

Islamic Republic of Iran

The Iran Islamic Revolutionary Guard Corps (IRGC) and the IRGC Quds Force (IRGC-QF), designated foreign terrorist organizations, utilize an expansive network of shell companies to avoid sanctions, exploit the U.S. financial system, and generate revenue to fund and support Iranian-backed terrorist groups, ballistic missile and nuclear weapons development, and the acquisition of a multitude of other defense articles and dual-use commodities for the Iranian regime.

HSI is well-positioned to address the Iran national security and public safety dangers through its global footprint, wide-ranging statutory authorities, and worldwide strategic partnerships. To counter these persistent and evolving threats, HSI launched an initiative focused on the illicit sales of Iranian-origin petroleum products violating U.S. and United Nations sanctions. To date, HSI and its partners have seized 4.8 million barrels of petroleum products aboard eight Iranian or IRGC-QF-associated tankers with an estimated value of \$289 million. Approximately \$11 million dollars of other assets related to the sale of IRGC petroleum were frozen by the Treasury Office of Foreign Assets Control and seized by HSI when the proceeds were discovered transiting the U.S. financial system. Additionally, HSI seized roughly \$35 million in currency from IRGC-QF-linked groups linked to the sale of oil products. It is estimated that the Iranian Government allocates \$5.1 billion to the IRGC from annual oil sales revenue. Based on these figures, HSI tanker seizures

have eroded over 4 percent of the IRGC yearly oil revenue allocation.⁸ Also, Iranian efforts to procure U.S. technology led to a 60 percent increase in Iranian tied HSI case initiations from FY 2022 to FY 2023.

In response to the Israel-Hamas conflict, HSI, under E2C2, initiated a working group of export enforcement agencies to address Hamas or Hezbollah procurement networks attempting to obtain U.S.-controlled commodities. The team comprises HSI; the Bureau of Industry and Security; U.S. Customs and Border Protection; the Department of State's Directorate of Defense Trade Controls; the Treasury Office of Foreign Assets Control; and the Department of Defense. This initiative employs a multi-prong approach, providing analytical support to agencies with current investigations, reviewing trade data to identify anomalies or suspicious patterns, and providing targeting insights within those regions' shipping networks.

Conclusion

HSI invests substantial effort and resources into export enforcement, even as illicit procurement networks become ever more resourceful in evading controls and sanctions. To overcome these challenges, HSI will continue to work with its export enforcement partners to combat foreign adversaries who seek to exploit American innovation and illegally acquire sensitive U.S. technology. Thank you for holding this important hearing, and I look forward to your questions.

⁸ Patrick Clawson, "Iran's Next Budget Assumes No Nuclear Deal," *The Washington Institute for Near East Policy Watch* 3558, (December 2021): para 9, <https://www.washingtoninstitute.org/policy-analysis/irans-next-budget-assumes-no-nuclear-deal>.

Post-Hearing Questions for the Record
Submitted to Kevin J. Kurland,
Deputy Assistant Secretary of Commerce for Export Enforcement
“Improving Export Controls Enforcement.”
Wednesday, April 10, 2024

From Senator Blumenthal

1. 15 C.F.R. § 772.1 defines knowledge for the purpose of the Export Administration Regulations (EAR) as: Knowledge of a circumstance (the term may be a variant, such as “know,” “reason to know,” or “reason to believe”) includes not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence. Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts. This definition does not apply to part 760 of the EAR (Restrictive Trade Practices or Boycotts).
 - a. Has the Bureau of Industry and Security (BIS) brought any enforcement actions where the conduct by the company in question evidenced “an awareness of a high probability of [the] existence or future occurrence” of a violation of the EAR, rather than positive knowledge?
 - b. If BIS has brought any such enforcement actions, have any such actions involved violations of regulations related to the Russia-Ukraine conflict? How many?
 - c. Please provide details regarding any such enforcement actions.

RESPONSE:

Preventing U.S. items from being exported or diverted through third countries to Russia is a top priority for Export Enforcement, and we have aggressively been using our authorities and partnerships, both domestically and internationally, to counter Russia's illicit procurement efforts. Since Russia's full-scale invasion of Ukraine, we have worked with our partners at the Department of Justice, FBI, and HSI to indict over a dozen Russian procurement networks. In addition to these criminal enforcement actions, we've issued more than 40 temporary denial orders and added more than 600 Russian entities and 250 parties in third countries to our Entity List. We have also established the Export Enforcement Five (E5) and Group of Seven (G7) Export Enforcement Sub-Working Group focused on countering Russian evasion, and we've published multiple guidance documents for industry related to Russia, including an E5 best practice document. Additionally, we have been reaching out to companies whose products have been identified in Russian weapons systems, including major distributors and global shippers, to identify and warn about possible diversionary actors in third countries, provide a recommended end-user certification form, and request that distribution agreements include heightened due diligence measures.

To date, BIS has brought criminal rather than administrative charges against those who have violated our Russia rules, although we have imposed temporary denial orders in coordination with certain of these criminal actions. Accordingly, we have not yet brought any enforcement actions based on “an awareness of a high probability of [the] existence or future occurrence” of a violation, although it is possible we would do so in the future. Even absent knowledge, BIS can impose administrative penalties based on strict liability.

2. In response to a question from Senator Romney concerning how many high-priority items are getting to our adversaries despite export controls, you noted that in the context of the semiconductor industry BIS has “issued over a dozen multi-sealed documents just in the past year and a half” aimed at “trying to get industry to harden their supply chains and their distribution networks.” Will you provide those documents to this Subcommittee and the Permanent Subcommittee on Investigations, which I chair?

RESPONSE:

The following list includes BIS, interagency, and international best practice documents aimed at hardening supply chains, including information on Common High Priority Codes coordinated with the European Union, Japan, and the United Kingdom:

Commerce, Justice, and Treasury Compliance Note on the Obligations of Foreign-Based Persons (March 2024); <https://www.justice.gov/opa/media/1341411/dl?inline>.

Russia Export Controls – List of Common High-Priority Items (February 2024); <https://www.bis.doc.gov/index.php/all-articles/13-policy-guidance/country-guidance/2172-russia-export-controls-list-of-common-high-priority-items>.

Department of Commerce, Department of the Treasury, Department of Justice, Department of State, and Department of Homeland Security Quint-Seal Compliance Note: Know Your Cargo: Reinforcing Best Practices to Ensure the Safe and Compliant Transport of Goods in Maritime and Other Forms of Transportation (December 2023); <https://ofac.treasury.gov/media/932391/download?inline>.

FinCEN and the U.S. Department of Commerce’s Bureau of Industry and Security Announce New Reporting Key Term and Highlight Red Flags Relating to Global Evasion of U.S. Export Controls (November 2023); https://www.fincen.gov/sites/default/files/shared/FinCEN_Joint_Note_US_Export_Controls_FINAL508.pdf.

Commerce, Justice, State, and Treasury Departments issue advisory on Iran ballistic missile procurement (October 2023); <https://www.justice.gov/d9/2023-10/2023-iran-ballistic-missile-procurement-advisory-10-17-final.pdf>.

Best Practice: Certification to Prevent Diversion to Russia of Highest Priority Items <https://www.bis.doc.gov/index.php/documents/policy-guidance/3339-tent-final-best-practice-customer-certification-v4/file>

Export Enforcement Five Guidance for Industry and Academia--Russia Sanctions--Common High Priority Items List (September 2023); <https://www.bis.doc.gov/index.php/documents/enforcement/3336-2023-09-26-export-enforcement-five-guidance-for-industry-and-academia-priority-hs-codes/file>.

Commerce, Justice, State, and Treasury Departments issue advisory providing guidance to industry on Iran's Unmanned Aerial Vehicle (UAV)-related activities (June 2023); <https://www.justice.gov/nsd/press-release/file/1586866/dl?inline>.

Commerce, Treasury, and Justice Compliance Note on Cracking Down on Third-Party Intermediaries to Evade Russia-Related Sanctions and Export Control (March 2023); <https://www.bis.doc.gov/index.php/documents/enforcement/3240-tri-seal-compliance-note/file>.

Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts (May 2023); <https://www.bis.doc.gov/index.php/documents/enforcement/3272-fincen-and-bis-joint-alert-final-508c/file>.

BIS Guidance to Exporters on Priority HS Codes (May 2023); <https://www.bis.doc.gov/index.php/documents/enforcement/3278-bis-guidance-to-prevent-evasion-of-prioritized-harmonized-system-codes-to-russia-final/file>.

FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts (June 2022); <https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf>.

3. In response to my questions regarding industry needing to do more to assist BIS in enforcing our export control efforts, you noted that you “personally, over the past 4 months, have signed out over 40 letters to the major distributors, manufacturers, and express carriers” regarding export controls. Will you provide those letters to this Subcommittee and the Permanent Subcommittee on Investigations?

RESPONSE:

As noted above, preventing U.S. items from being exported or diverted through third countries to Russia is a top priority for Export Enforcement, and we have aggressively been using our authorities and partnerships, both domestically and internationally, to counter Russia's illicit procurement efforts. As part of this effort, we have been reaching out to companies whose products have been identified in Russian weapons systems, including major distributors and global shippers.

To date, Export Enforcement has issued more than 40 letters to such companies. The letters identify and warn companies about possible diversionary actors in third countries, provide a recommended end-user certification form, and request that distribution agreements include heightened due diligence measures. BIS stands willing to work with this Subcommittee and the Permanent Subcommittee on Investigations on any request for information.

From Senator Scott (FL)

1. Mr. Kurland, part of our policy priorities must be stopping China's nonmarket economic practices and making sure their companies are curtailed from becoming global leaders and their industries from gaining global monopolies when propped up by the CCP. One particular case of this is the drone industry. Thankfully, my American Security Drone Act (ASDA) is now law to help address this concern of China's control of 80% of the global drone market. But other American and allied technology industries have similar concerns about how their companies compete with China's global giants, like Huawei. Does the Department consider Chinese competitors to U.S. businesses and the global competition landscape when making export control decisions to other countries that are not China? How does the Bureau enforce compliance with restrictions and licenses in sensitive areas and also assess where there may need to be opportunities for exporting to provide a market alternative to a Chinese product in another country outside of China?

RESPONSE:

The 2024 Intelligence Community Annual Threat Assessment identifies nation-state actors, including the People's Republic of China (PRC), as among the most pressing threats to our national security. Accordingly, preventing and deterring the PRC from illicitly acquiring U.S. technology to support its military modernization efforts and enable human rights abuses is a top priority of Export Enforcement. To combat the malign intentions of the PRC and other nation-state actors, BIS and the Department of Justice established the Disruptive Technology Strike Force last year to leverage the resources and authorities of the U.S. Government to prioritize enforcement outcomes involving export control violations of our most sensitive technologies. To date, the Strike Force has announced 16 cases, including six involving China. For example, in March 2024, a federal grand jury indicted Linwei Ding, aka Leon Ding, charging him with four counts of theft of trade secrets in connection with an alleged plan to steal proprietary information related to artificial intelligence technology from Google (see <https://www.justice.gov/opa/pr/chinese-national-residing-california-arrested-theft-artificial-intelligence-related-trade>). The Strike Force has also leveraged BIS's unique administrative enforcement and regulatory authorities. For example, on May 9, BIS added 37 parties to the Entity List for their involvement in the PRC's quantum, drone, and high-altitude balloon programs as part of a Strike Force action.

Export Enforcement's role in the licensing process, including for PRC transactions, is to identify vulnerabilities related to the diversion or misuse of technology by unauthorized parties or end uses, and related enforcement interests to inform the BIS position on whether to approve or deny a license application; it does not consider competitors to U.S. businesses and the global competition in its recommendations to Export Administration. Similarly, Export Enforcement does not consider export opportunities when investigating violations of the EAR, including restrictions on sensitive items.

2. Late last year, Commerce Secretary Gina Raimondo called for increased resources for the Commerce Department's Bureau of Industry and Security (BIS) to pursue a "very aggressive, innovative approach" against China aimed at denying China's ability to catch up on cutting-edge semiconductors. Despite this rhetoric, it was recently brought to my attention that the U.S. Government is still allowing American companies to sell chips to Huawei, a Chinese company that has been identified as a national security risk to the U.S. and added to the Entity List. Typically, adding a company to the Entity List has served as a death sentence. To the contrary, at the end of the Trump Administration, Commerce issued an exclusive monopoly license to one American chip company to sell 4G mobile logic chips to Huawei. To date, it has been the Biden Administration's policy to deny issuing further licenses to American companies to sell to Huawei. In fact, it was publicly reported by the Wall Street Journal in early 2023 that BIS was planning to revoke export licenses issued to U.S. suppliers for sales to Huawei, according to an interview given by BIS Under Secretary Alan Estevez. However, more than one year later, the licenses have yet to be revoked as outlined in a March 12 Reuters article highlighting that both Intel and Qualcomm still hold exclusive licenses to sell chips to Huawei for tablets and cellphones, respectively. Further, an April 3 article by Light Reading specifically calls attention to how Huawei's resurrection is the result of these BIS-enabled monopoly licenses. I remain incredibly concerned that these older monopoly licenses still exist, especially while the U.S. Government continues "rip and replace" efforts aimed at removing Huawei from U.S. networks and attempts to persuade our allies to do the same.
 - a. Some estimates suggest that nearly 90 percent of all of Huawei's phones have exclusively U.S.-designed Qualcomm chips in them. Why are we still allowing U.S. companies to sell semiconductor chips to Huawei?

RESPONSE:

Export Enforcement aggressively enforces controls on items subject to the EAR to parties on the Entity List, including Huawei Technologies Co., Ltd. (Huawei). For example, last April, Export Enforcement 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. 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. In addition, in November 2021, Export Enforcement imposed an \$80,000 penalty against SP Industries for violating the Huawei Entity List restrictions and required the company to complete audits of its export compliance program.

I work on the Export Enforcement side of the organization, and our input to the licensing process is to prevent the diversion to or misuse of technology by unauthorized parties or end uses. However, I understand that the policy side of BIS is engaging in an ongoing assessment of our export control policies related to the PRC, including the existing licensing policy for license applications involving Huawei, and calibrating them based on the evolving threat environment. As part of this process, as it has done in the past, BIS sometimes revokes export licenses. Although I am unable to comment on specific licenses, it has been publicly reported that, on May 7, 2024, BIS revoked certain licenses for exports to Huawei.

- b. Isn't this allowing Huawei to sustain and expand its mobile phone business and compete with the other phone companies who are not on the Entity List? Doesn't this undermine the government's interest in rewarding compliance?

RESPONSE:

I work on the Export Enforcement side of the organization, and our input to the licensing process is to prevent the diversion to or misuse of technology by unauthorized parties or end uses. However, I understand that the policy side of BIS is engaging in an ongoing assessment of our export control policies related to the PRC, including the existing licensing policy for license applications involving Huawei, and calibrating them based on the evolving threat environment. As part of this process, as it has done in the past, BIS sometimes revokes export licenses. Although I am unable to comment on specific licenses, it has been publicly reported that, on May 7, 2024, BIS revoked certain licenses for exports to Huawei.

3. If the average approval duration for a license is four years, how many active licenses do you have in Communist China at any given time, Mr. Kurland?

RESPONSE:

BIS is constantly reviewing and calibrating its controls on the PRC to restrict access to U.S. items that would advance its military modernization efforts or enable human rights abuses. At Export Enforcement, our goal is to prevent and deter the PRC from illicitly acquiring U.S. items through aggressive enforcement, including in partnership with other federal law enforcement agencies through the Disruptive Technology Strike Force.

While I work on the Export Enforcement side of the organization, not the licensing side, my understanding is that during the four-year period from May 17, 2020 to May 17, 2024, BIS processed 20,438 licenses involving the Peoples Republic of China (PRC) as the ultimate destination country. Of these, 14,401 (70 percent) were approved, 4,748 (23 percent) were returned without action, and 1,237 (6 percent) were denied. Given the general four-year license validity period, it is likely that there are currently around 14,000 active licenses authorizing exports to the PRC.

4. We know that for certain actions and petitions, the Commerce Department presumes injury for U.S. businesses. What sort of presumptions exist for the items that the U.S. Government is worried about sharing with other actors in foreign countries – including Communist China – that are on the Commerce Control List? Are there certain items on the list that we presume should not be given a license for export to Communist China?

RESPONSE:

I help lead the enforcement side of BIS, not the licensing side. Export Enforcement's mission is laser-focused on preventing any technology, whether or not on the Commerce Control List (CCL), from being misused, especially by nation-state actors like China, Russia, Iran, and North Korea. Specifically, Export Enforcement provides input to the licensing process and reviews unlicensed transactions to prevent and disrupt the diversion to or misuse of any items by unauthorized parties or for unauthorized end uses like destabilizing military modernization efforts (including weapons of mass destruction) or enabling human rights abuses. As a result of

its aggressive enforcement posture, last fiscal year, for example, Export Enforcement actions resulted in the highest number of criminal convictions and administrative actions in our history, including the largest standalone administrative penalty ever (\$300 million). We also established the Disruptive Technology Strike Force with the Department of Justice to leverage the resources and authorities of the U.S. Government to prioritize enforcement outcomes involving export control violations of our most sensitive technologies, whether or not on the CCL. Additionally, Export Enforcement identifies foreign parties for addition to the Entity List, which can result in the imposition of a license requirement for any items subject to the EAR often subject to a policy of denial. By using a combination of our criminal and administrative enforcement authority along with regulatory actions like license reviews and Entity Listings, BIS works to prevent and deter the misuse of all EAR items.

5. Mr. Kurland, has Communist China ever successfully sued the Commerce Department and had any of its companies removed from the Entity List?

RESPONSE: To date, no decision to place an entity on the Entity List has been reversed through litigation.

6. Commerce utilizes the Automated Export System, “AES” which enables relatively efficient and real-time data tracking. Over time, however, decisions have been made to share less information with the public and Congress. Will BIS commit to sharing data with Congress on a regular basis derived from the AES and regarding what has been exported, to where, and if it is subject to a license or not?

RESPONSE: BIS is committed to sharing information with Congress to the fullest extent authorized by the Export Control Reform Act of 2018 (ECRA). This includes: monthly meetings with our authorizing committee staff at the Deputy Assistant Secretary level; briefings upon request – including recent briefings provided to staff from the Homeland Security & Government Affairs’ Permanent Subcommittee on Investigations on our Russia enforcement actions; responses to congressional letters; and responses to formal requests from chairs or ranking members. As to specific AES data, BIS is prohibited from disclosing information in connection with exports of items under Commerce jurisdiction by section 1761(h) of ECRA (50 U.S.C. 4820(h)) absent a written request on letterhead of a chair or ranking member of a Congressional committee or subcommittee of appropriate jurisdiction.