

**ADVANCING NATIONAL SECURITY THROUGH EX-
PORT CONTROLS, INVESTMENT SECURITY, AND
THE DEFENSE PRODUCTION ACT**

HEARING
BEFORE THE
COMMITTEE ON
BANKING, HOUSING, AND URBAN AFFAIRS
UNITED STATES SENATE
ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

ON

EXAMINING HOW TO COORDINATE EXPORT CONTROLS AND INVEST-
MENT SECURITY POLICIES AND WHAT STEPS CONGRESS CAN TAKE
TO STRENGTHEN THESE AUTHORITIES

JULY 25, 2024

Printed for the use of the Committee on Banking, Housing, and Urban Affairs



Available at: <https://www.govinfo.gov/>

U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

SHERROD BROWN, Ohio, *Chair*

| | |
|---------------------------------|-----------------------------|
| JACK REED, Rhode Island | TIM SCOTT, South Carolina |
| ROBERT MENENDEZ, New Jersey | MIKE CRAPO, Idaho |
| JON TESTER, Montana | MIKE ROUNDS, South Dakota |
| MARK R. WARNER, Virginia | THOM TILLIS, North Carolina |
| ELIZABETH WARREN, Massachusetts | JOHN KENNEDY, Louisiana |
| CHRIS VAN HOLLEN, Maryland | BILL HAGERTY, Tennessee |
| CATHERINE CORTEZ MASTO, Nevada | CYNTHIA M. LUMMIS, Wyoming |
| TINA SMITH, Minnesota | J.D. VANCE, Ohio |
| RAPHAEL G. WARNOCK, Georgia | KATIE BOYD BRITT, Alabama |
| JOHN FETTERMAN, Pennsylvania | KEVIN CRAMER, North Dakota |
| LAPHONZA R. BUTLER, California | STEVE DAINES, Montana |

Laura Swanson, *Staff Director*

Lila Nieves-Lee, *Republican Staff Director*

Elisha Tuku, *Chief Counsel*

Cameron Ricker, *Chief Clerk*

Shelvin Simmons, *IT Director*

Pat Lally, *Assistant Clerk*

C O N T E N T S

THURSDAY, JULY 25, 2024

| | Page |
|--|------|
| Opening statement of Chair Brown | 1 |
| Prepared statement | 28 |
| Opening statements, comments, or prepared statements of: | |
| Senator Scott | 3 |
| Prepared statement | 29 |

WITNESSES

| | |
|--|----|
| Thea Kendler, Assistant Secretary for Export Administration, Department of Commerce | 5 |
| Prepared statement | 30 |
| Responses to written questions of: | |
| Chair Brown | 48 |
| Senator Scott | 50 |
| Paul Rosen, Assistant Secretary for Investment Security, Department of the Treasury | 6 |
| Prepared statement | 37 |
| Responses to written questions of: | |
| Senator Scott | 72 |
| Senator Warren | 79 |
| Senator Fetterman | 80 |
| Grant Harris, Assistant Secretary for Industry and Analysis, Department of Commerce | 8 |
| Prepared statement | 39 |
| Responses to written questions of: | |
| Senator Scott | 82 |
| Senator Warren | 85 |
| Senator Fetterman | 86 |
| Laura Taylor-Kale, Assistant Secretary for Industrial Base Policy, Department of Defense | 9 |
| Prepared statement | 43 |
| Responses to written questions of: | |
| Senator Scott | 89 |

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

| | |
|--|----|
| U.S. Department of State denial document | 90 |
| Letter submitted by MGS | 97 |

ADVANCING NATIONAL SECURITY THROUGH EXPORT CONTROLS, INVESTMENT SECURITY, AND THE DEFENSE PRODUCTION ACT

THURSDAY, JULY 25, 2024

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Committee met at 10 a.m., via Webex and in room 538, Dirksen Senate Office Building, Hon. Sherrod Brown, Chair of the Committee, presiding.

OPENING STATEMENT OF CHAIR SHERROD BROWN

Chair BROWN. The Senate Committee on Banking, Housing, and Urban Affairs will come to order.

Welcome to our witnesses. We face an uncertain world with many geopolitical challenges from Russia's continued brutal invasion of Ukraine to ongoing conflicts in the Middle East to an increasingly aggressive and capable Chinese military. We know that China has built that military capability with the help of some of America's biggest corporations and even American tax dollars.

For too long, our Government was willfully blind to the threat China posed. Multinational corporations eager to move jobs wherever they could pay ever-lower wages lobbied this body—and Presidents of both parties failed us—for permanent normal trade relations with China. When corporations moved products overseas, they outsourced the technology and the trade secrets along with it. We did nothing to stop it, and now we are paying the price.

We can't make the kinds of mistakes we have in the past. We have to be proactive about these threats and take action now to protect our national and economic security. And we need to be clear: those two issues are intimately connected. You can't separate the economy and our national security.

Today hostile Governments work together more and more to challenge the interests and the securities and the values of the United States, our allies, and partners around the world. Increasingly, hostile Governments use our own technology to fuel their destructive efforts. We must lead efforts to stop it.

It is the U.S. Government's job to police the flow of sensitive and so-called "dual use technologies"—technologies that can be used for both military and civilian purposes. The Departments of Commerce and Treasury, along with DoD, State, and other agencies, try to restrict the flow of sensitive technologies to our adversaries. We can't allow U.S. innovation and investments to be used against us.

Against that backdrop, NATO met earlier this month. They issued a statement addressing these threats. Specifically, NATO leaders called on China to “cease all material and political support to Russia’s war effort” including “the transfer of dual-use materials, such as weapons components, equipment, and raw materials that serve as inputs for Russia’s defense sector.” That was the NATO statement.

That followed last month’s G7 Summit in Italy where the United States and our allies reaffirmed our shared efforts to implement export controls to a risk—address risks to international security and “to ensure the effectiveness of our respective foreign investment screening.” The G7 leaders also noted that measures designed to address risks from outbound investments could be important to complement existing tools of targeted controls on exports and outbound investments.

A core element of this Committee’s work has been to establish and conduct oversight over our export controls, investment security, and Defense Production Act authorities. Treasury and Commerce have had active and growing caseloads since our hearing last year.

They have expanded controls on semiconductors, equipment, and services that could support China’s semiconductor ecosystem. They have taken steps to establish an outbound investment program that would enable us to better understand—and to stop—U.S. investments that buildup China’s military.

They have recently issued a proposed rule that would significantly expand the Committee on Foreign Investment in the U.S.’s ability to review foreign real estate investments near military bases, like Wright-Patterson Air Force Base in Ohio. It is the kind of action I and many from both parties have been pressing for. I hear from farmers in Ohio near our military installations who are very concerned about this.

As we use our export control and investment security policies to restrict China’s ability to use U.S. technology and investments to advance their military capabilities and human rights abuses, we must also bolster our own domestic capabilities. To that end, I was pleased to see Dr. Taylor-Kale and her colleagues—thank you—release the Defense Department’s first ever National Defense Industrial Strategy earlier this year. As a critical economic security tool, this Committee has jurisdiction over the Defense Production Act, which must play a vital role in advancing that strategy.

In Ohio, we know the potential here to harness the talents and patriotism of America’s workers to protect our country. For decades, the Air Force Research Lab at Wright Patterson Air Force Base near Dayton has been the home of the DPA Title III program. Aside from the good work being done at AFRL, the Defense Production Act gives the Administration the authority to allocate and prioritize critical materials and to increase domestic productive capacity to address industrial shortfalls.

In other words, the DPA allows the Defense Department and other agencies to invest in American manufacturing that can support U.S. national security as well as making us more prepared for emergencies. This work couldn’t be more urgent.

For decades, corporate offshoring and consolidation and restructuring—essentially just another elite business school term for finding new ways to screw workers to increase profits—all weakened our domestic manufacturing sector. Let me say that again. For decades, corporate offshoring, consolidation, and restructuring, all with the aid and assistance of too many members of this body, all weakened our domestic manufacturing sector.

Ohioans know well what it has done to cities like where I grew up, Mansfield, our families, our economy. Increasingly, people in this town finally are waking up to how it has weakened our national security. We know when companies outsource jobs they outsource technologies capabilities with them.

There has not been enough appreciation for how much innovation happens on the production floor by workers. Over the past few years, we have finally taken steps to reverse that course, passing CHIPS and Science Act, passing the Bipartisan Infrastructure Law. We have increased funding for strategic investments using the Defense Production Act. We can do more.

As Congress prepares to reauthorize the Defense Production Act, we need to look at new ways the DPA can support American industrial capabilities and help us revitalize our domestic industrial base to meet current and future challenges.

Today we will discuss how we are working with our partners to coordinate our export controls and investment security policies and what steps Congress can take to strengthen these authorities.

We look forward to testimony from this panel, who can update the Committee on their important work.

Senator Scott.

OPENING STATEMENT OF SENATOR TIM SCOTT

Senator SCOTT. Thank you, Mr. Chairman. I would like to start by reminding this room and our witnesses of the important role they play in safeguarding our Nation's economic and national security priorities.

President Reagan once rightly noted that we are in a different world, and our defenses must be based on recognition and awareness to combat our enemies of the modern day. While he was talking about the Soviets, unfortunately, many of our adversaries remain the same: Russia, China, Iran, and North Korea.

But, thankfully, what also remains the same is the American spirit to innovate and to create the world's leading technologies. My own State of South Carolina is an excellent example. From F-16s to the world's best luxury airliners to leading automotive manufacturing to creating next-generation technologies, I would say South Carolina is simply our future.

But to safeguard that future we must ensure that policies created here in Washington don't cutoff growth and stifle future innovation. We must have a global economy where America is the leader. After more than 3 years of President Biden's policies, we have seen soaring inflation that is crushing every day Americans, wars across our globe, and our enemies challenging us and our allies at every single turn. We can, and we must frankly, do better.

So today as we discuss and evaluate some of our economic national security tools, our export controls, investment security, and

the Defense Production Act, we must keep these principles in mind. At times, we must be willing to reassess our policies and retool our positions. And, frankly, let's consider our allies.

One thing we certainly learned through COVID was depending on China is a really bad strategy. To be effective in countering China, we must work with our allies, so that China cannot easily find workarounds to our U.S. export controls by simply buying these same technologies and equipment from our friends.

A failure to look holistically at our economic strategy can and will damage American security, competitiveness, and unfairly leave U.S.-led industry behind.

In fact, a recent study by the New York Federal Reserve found that the Biden administration's export control policies on the semiconductor industry have led to decreased profitability, job losses, and \$130 billion in financial loss across the industry. With new reports that these types of policies have directly led to thousands of layoffs in States ranging from Ohio to New York, we must scrutinize the actions leading to these results. But it doesn't stop there.

In my home State of South Carolina, recent actions by the Commerce Department to revoke thousands of export licenses for gun manufacturers have resulted in millions of dollars in losses. I have sent three letters to the Commerce Department on this issue, and now reports suggest that we will see over \$500 million in annual losses across U.S. firearms manufacturers.

Mr. Chairman, I have a letter here that I would like to submit for the record.

Chair BROWN. Without objection, so ordered.

Senator SCOTT. Thank you, Mr. Chairman. In my home State of South Carolina, a small minority-owned firearms business had more than \$71 million worth of export licenses revoked by the Biden Commerce Department. Unfortunately, this meant that the firm defaulted on multiple international contracts, and now those same contracts are being backfilled by China and others. And it is my understanding that these licenses were revoked for foreign policy reasons such as furtherance of world peace.

So instead of supporting American companies, we just handed over the marketplace to China. Export controls, investment security, and important tools like the Defense Production Act, should be used in a responsible manner that maximizes growth here at home and economic pain for our adversaries. I strongly believe that when we have a better domestic environment, a better ability to innovate and manufacture, that means that America is winning.

Thank you, and I look forward to discussing these important issues with our witnesses.

Chair BROWN. Thank you, Senator Scott.

Our witnesses today, two of them have been in front of our Committee before. Two are new witnesses. Thank you for joining us.

Thea Kendler is Assistant Secretary for Export Administration at the Commerce Department. Paul Rosen is Assistant Secretary for Investment Security, Department of the Treasury. Grant Harris, Assistant Secretary for Industry and Analysis, Department of Commerce. Dr. Laura Taylor-Kale is the Assistant Secretary for Industrial Base Police at Department of Defense.

Thank you—all four of you—for your public service, and welcome, and you are recognized, Ms. Kendler.

STATEMENT OF THEA KENDLER, ASSISTANT SECRETARY FOR EXPORT ADMINISTRATION, DEPARTMENT OF COMMERCE

Ms. KENDLER. Thank you, Chairman Brown, Ranking Member Scott, distinguished Members of this Committee. Thank you for inviting me to testify about the Biden-Harris administration's ongoing efforts to administer export controls and protection of U.S. national security interests.

I appreciate the opportunity to work together with you to ensure we are effectively countering China's military modernization and human rights abuses, degrading Russia's ability to wage war on Ukraine, identifying and controlling technologies that are critical to our national security, and collaborating with our allies and partners in these efforts.

BIS does not take on these tasks alone. License applications and licensing policy are adjudicated and set together with the Departments of Commerce, Defense, Energy, and State. Our greatest priority is to effectively apply export controls to thwart China's military modernization efforts.

We know that China is going to great lengths to obtain key U.S. advanced technologies with military potential, and we are responding accordingly as demonstrated by our October 2022 and 2023 advanced computing controls. These restrictions aim to impede China's ability to develop artificial intelligence systems used for the development of advanced weapons systems, malicious cyber activity, and other military and intelligence applications.

With our interagency partners, we closely scrutinize license applications to the PRC focusing on end users and end uses as well as risk of diversion to unauthorized activities. We are not afraid to take the time we need to carefully analyze applications involving PRC parties to assess any and all risks to U.S. national security and foreign policy.

Just this morning we released new proposals to expand restrictions on exports and the provision of support to military intelligence and foreign security end users and end uses consistent with the fiscal year 2023 NDAA. This includes controls on U.S. person support to such activities in China.

And last week we took action to ensure strong U.S. leadership in the development of standards for critical and emerging technologies. Through an export controls rulemaking, we enabled increased U.S. private sector participation in standard-setting organizations. This undercuts any advantage China could establish in the absence of U.S. industry participation.

At the same time, our commitment to working with allies and partners on export controls has never been stronger. Export controls are more effective when used in concert with our partners and allies. We are in the process of finalizing controls now on new critical and emerging technologies, including quantum, and some of our allies and partners have already taken parallel action. We continue to surge forward in common controls against Russia with our 38 global export control coalition partners.

Earlier this month I was in Brussels meeting with counterparts from the European Commission, Japan, and the United Kingdom, to discuss combined efforts to enhance the controls we imposed on Russia in response to its attacks on Ukraine. We have also coordinated outreach to third countries outside of our coalition to more forcefully combat illegal diversion.

Alongside our tireless commitment to control the export of U.S. technologies, BIS is deeply dedicated to ensuring the health of our Defense Industrial Base. Through the critical tools provided by the Defense Production Act, we work alongside interagency partners to ensure that critical Department of Defense and emergency procurement needs are met.

Our DPA authorities also enable us to issue highly confidential and bespoke surveys to industry participants informing our use of export controls and interagency approaches to national security issues. Reauthorization of the DPA is critical for BIS's support to our Defense Industrial Base.

Dual-use export controls have never been more necessary to our national security. We, in Export Administration at the Commerce Department, are focused on aggressively contending with the national security threats facing our country and using all the tools at our disposal to ensure we maintain U.S. technological leadership in furtherance of national security.

Finally, while I recognize that this is not an appropriations committee, I urge you to support additional funding for BIS. We are facing more sophisticated threats from China, Russia, and Iran, rapid advances in technology, increasing complexity of export license applications, and more and more critical and emerging technologies subject to our controls. To outpace these threats, we need to resource our mission appropriately.

Thank you. I welcome your questions.

Chair BROWN. Thank you, Assistant Secretary Thea.

Thank you, Secretary Rosen.

STATEMENT OF PAUL ROSEN, ASSISTANT SECRETARY FOR INVESTMENT SECURITY, DEPARTMENT OF THE TREASURY

Mr. ROSEN. Chairman Brown, good morning. Ranking Member Scott, good morning, and Members of the Committee. Thank you for the opportunity to provide an update on the work of the Department of the Treasury's Office of Investment Security and the Committee on Foreign Investment in the United States or CFIUS.

I also want to thank Congress for the authorities and resources you have provided since the passage of the Foreign Investment Risk Review Modernization Act of 2018, or FIRRMA, as well as the constructive and bipartisan support you have provided to our national security mission, which has helped make possible many of the enhancements I will discuss here today.

Last year I spoke to this Committee about our work and the progress we have made to safeguard national security, and today I would like to update you on these efforts, which have been extensive and ongoing. Over the past 18 months, we have strengthened our analytical and operational capabilities by building and implementing sophisticated tools, platforms, and methodologies for assessing and addressing national security risks, employing cutting

edge information technology platforms to securely manage and facilitate novel aspects of CFIUS's work and expanding and deepening our human capital to build a team with diverse backgrounds.

These improvements have enabled us to be more efficient and effective, even as we contend with two core challenges. Transactions are becoming more complex and sophisticated in their structures, and CFIUS is identifying and addressing more national security risks than in years past. We have paid particular attention to the role of limited partners in investment funds, as their access to, influence, and control over sensitive businesses can vary considerably.

All while tackling these challenges, Treasury has successfully improved the efficiency of CFIUS's operations. As noted in the latest annual report, in 2023, CFIUS cleared 66 percent of filed declarations or notices within the first 30 or 45 days, respectively, compared to 58 percent in 2022.

The rate at which parties withdrew and refiled their notices also declined from 23 percent to 18 percent, the first such decrease in 5 years. These changes are not incidental but reflect improved efficiencies, which is a cornerstone of our focus.

Treasury has also transformed the way the Committee approaches compliance with mitigation agreements and enforcement thereof. We have expanded and devoted significant resources to the monitoring and enforcement mission, including by nearly doubling the size of Treasury's team over the last several years.

We have also continued to enforce violations of mitigation agreements, where appropriate. In fact, in 2023, CFIUS imposed four civil monetary penalties for violations of material provisions of mitigation agreements, which was double the number of civil monetary penalties that CFIUS had previously imposed in nearly its 50-year history. CFIUS has also for the first time issued subpoenas pursuant to its authority to execute its national security mission.

We have expanded our efforts to identify transactions that were not notified to the Committee voluntarily and that may pose a risk to national security. The Committee leverages multiple tools to identify and analyze such non-notified transactions. And Treasury's non-notified team screens thousands of potential covered transactions, ultimately putting forward to the Committee for consideration to request to file those transactions that may pose a national security risk or issues.

The MineOne transaction that President Biden blocked earlier this year came to the Committee from—through the non-notified process in the form of a public tip. Treasury has also led a number of regulatory enhancements to CFIUS authorities over these years. Working with our partners at the Department of Defense, Treasury issued a proposed rule this month to significantly bolster CFIUS's jurisdiction over real estate transactions. We are also working to finalize the proposed rule to sharpen our investigation and enforcement tools.

In many instances, our tools work best when we collaborate and act with our allies and partners. And, in 2023 and 2024, CFIUS had more than 300 engagements with allies and partners. And, since 2019, approximately 30 countries have proposed, enacted, or

significantly expanded their foreign investment review regimes with our support.

And, last, let me update you briefly on Treasury's efforts to implement President Biden's Outbound Investment Security Program. Treasury issued a proposed rule last month for this program, and my office is working closely with the interagency to review comments and prepare a final report.

This important program's success ultimately will depend on the resources we receive, and to that end I would ask Congress to fully support Treasury's request in the President's 2025 budget for this program at 16.7 million.

Thank you, and I look forward to your questions.

Chair BROWN. Thank you, sir. Thank you, Secretary Rosen.

Secretary Harris, welcome.

**STATEMENT OF GRANT HARRIS, ASSISTANT SECRETARY FOR
INDUSTRY AND ANALYSIS, DEPARTMENT OF COMMERCE**

Mr. HARRIS. Chairman Brown, Ranking Member Scott, distinguished Members of the Committee, thank you for inviting me to testify today.

As Assistant Secretary of Commerce for Industry and Analysis, I lead a team of over 265 industry experts and economists. Our mission is to support the global competitiveness of U.S. industry. This unit, which sits in the International Trade Administration, is the analytical engine of U.S. competitiveness policy, because it is the broadest industry expertise available in any one place in the U.S. Government.

We cover approximately 90 percent of the U.S. economy and work on everything from raw materials like critical minerals to vital components like semiconductors, to finished goods like autos and airplanes. The unit's singular industry expertise, our unique commercial perspective, and our advanced analytics capabilities are critical to advancing U.S. Government work on outbound investments, CFIUS, and supply chain resilience.

With respect to outbound, Commerce plays a special role in supporting the program. Commerce is key to identifying and understanding the relevant technologies to be covered and how their requirements should be scoped. We have the technical fluency and industry relationships to help anticipate the national security risks that may be associated with cutting edge technologies.

In addition, my team has spearheaded extensive industry engagement, consulting over 450 stakeholders, working with Treasury as the development of the program has progressed. This is important as we seek to craft an effective program while reducing the risks of unintended market effects.

Commerce will also be key to successful implementation. Our sector-specific experts will be indispensable to interpreting and recommending action based on analysis of the data received through the program.

Turning to CFIUS, the industry and analysis unit leads Commerce's participation in the Committee and analyzes issues related to the U.S. business and the market in which it operates, market trends, and the business rationales for transactions, among other

issues. My team works closely with colleagues across the Department, especially in BIS.

In 2022, President Biden directed CFIUS to consider supply chain resiliency in its national security reviews. Commerce analyzes issues such as the scale and types of supply relationships pertaining to a given U.S. company and the potential for supply chain disruptions or undue foreign influence over specific supply chains.

More broadly on supply chains, the industry and analysis unit has long been central to U.S. supply chain work. We have had a supply chain services-focused office for over a decade, and for years before that a dedicated team.

We focus on applied analysis and action. For instance, the industry and analysis unit was the first team in the U.S. Government to sound the alarm on competitiveness in the semiconductor supply chain and spring into action. The team mapped out chokepoints, created an early warning system, and connected industry leaders with suppliers to encourage solutions.

The team also set to work supporting investments to strengthen the supply chain and was recognized for securing investments into the United States totaling \$34 billion and supporting over 20,000 U.S. jobs.

Last year we established what the White House called a first-of-its-kind supply chain center. We are pioneering new data-driven tools and creating playbooks to assess supply chain vulnerabilities in specific sectors, including for emerging technologies. Our supply chain exposure tool provides a common operating picture that enables evidence based actions with international partners.

We are also building a diagnostic tool to assess supply chain risk across the U.S. economy with an emphasis on risks to national security and economic security most relevant to the U.S. Government.

In conclusion, the industry and analysis unit's industry expertise is vital to investment security, U.S. technological leadership, supporting domestic manufacturing and job growth, and addressing unfair trade practices by the People's Republic of China.

The President's fiscal year 2025 budget request for the International Trade Administration includes \$5 million in new funding to support the Outbound Investment Security Program, and \$12 million to support our supply chain work. In finalizing the fiscal year 2025 appropriation bills, we ask that you please consider how important it is for U.S. national security to support and fund these functions.

Thank you, and I look forward to answering your questions.

Chair BROWN. Thank you, Mr. Secretary.

Secretary Taylor-Kale, welcome.

STATEMENT OF LAURA TAYLOR-KALE, ASSISTANT SECRETARY FOR INDUSTRIAL BASE POLICY, DEPARTMENT OF DEFENSE

Ms. TAYLOR-KALE. Thank you. Good morning, Chairman Brown, Ranking Member Scott, and distinguished Members of the Committee. I am grateful for this opportunity to represent the Department of Defense today.

As the first Senate-confirmed Assistant Secretary of Defense for Industrial Base Policy, issues of national security and issues of eco-

conomic security interlink for us in the Department of Defense. Generally, I interact with the Armed Services Committee. However, this Committee has oversight over key areas of economic security that are of critical importance to DoD—CFIUS, antitrust reviews, and the Defense Production Act, in particular.

Through DoD’s role on CFIUS, we see how adversarial capital investments in the U.S. technological base attempt to weaken the United States by robbing us of our technological know-how. Our role in Hart-Scott-Rodino antitrust reviews allows the DoD to remain vigilant to adversaries using unfair trade and predatory acquisition and investment strategies to weaken the U.S. Defense Industrial Base. All of these remain very important priorities for the Department of Defense as underscored in the National Defense Industrial Strategy, in support of economic deterrence, and our warfighters.

And while I welcome questions on any of these topics, today I will focus most of my comments on the Defense Production Act. The Defense Production Act expires in September 2025, and the Department of Defense strongly supports a 5-year reauthorization of DPA and believes that the reauthorization needs to happen this year in the NDAA or another means rather than risk a lapse of authorities by waiting until 2025.

Why is that? Because in addition to timely, consistent appropriations and multiyear procurement authority, supporting the Defense Production Act may be one of the most important actions that Congress can take to ensure that the U.S. Industrial Base is ready to preserve our military advantage and support the warfighter.

I would also like to take this opportunity to thank Congress for expanding the definition of “domestic source” in the Defense Production Act to include Australia and the United Kingdom. This allows us to, in addition to working with Canada, to support and work with our allies and partners to strengthen our own industrial base as well.

DoD’s primary aim in the use of the Defense Production Act is to increase the readiness and resilience of the Defense Industrial Base in support of defense critical needs and the warfighter.

Since Congress enacted the DPA in 1950, the Executive branch has invoked DPA authorities to manage the Nation’s defense-related production capacity, our critical supply chains, and to protect and strengthen the U.S. industrial base in times of war, peace, and national emergencies. And today it remains an essential national defense tool.

Make no mistake, our adversaries attempt to use supply chain vulnerabilities to weaken the U.S. economy and our military, and the DPA remains one of the most effective tools to bolster our domestic industrial production.

We use the DPA Title I prioritize components for defense systems and ensure availability of components does not preclude industry from delivering warfighter needs in a timely and costly—cost effective manner. We use Title III to alleviate pain points in supply chains and expand domestic manufacturing of critical technologies and processing and production of critical minerals and strategic materials.

Since the last reauthorization in 2018, DoD appropriations for DPA Title III have increased dramatically from an average of \$70 million a year to about \$750 million a year.

Last fiscal year, we executed over \$733 million of DPA Title III awards in micro-electronics, strategic and critical minerals, kinetic capabilities, energy storage, and batteries. Going forward, we need to do more. And, yes, Senator Scott, we also need to do so responsibly.

We recently announced a Defense Industrial Base Other Transaction Authorities, a consortium that will allow DoD to expand execution of DPA awards more timely and offer more small businesses and companies that are not traditionally part of the Defense Industrial Base to compete for awards.

We continue to want to work with allies and partners through security of supply arrangements, and of course now that we can work with Australia and—Australian and U.K. companies as well in support of AUKUS and other secure—in order to secure defense critical supply chains.

As Congress considers reauthorization, we recommend a few changes to the DPA law, including raising the DPA fund balance to allow that annual fund balance to increase, so that appropriations won't be penalized, and we would like to create more executive offices in addition to our great partnership with the good people of Ohio who work for AFRL.

We also support increasing the period of availability of funds, which will allow the Department to support advance procurement of material for defense critical components.

Again, I am absolutely honored to be here today representing the Department of Defense, and ultimately I hope that our joint efforts will continue to ensure the necessary resources for our warfighters and secure our Nation's economic future.

Thank you again.

Chair BROWN. Thank you, Secretary Taylor-Kale.

I will begin the questioning with Senator Cortez Masto of Nevada.

Senator CORTEZ MASTO. Thank you, Mr. Chairman. And thank you to the Ranking Member for the hearing today.

Assistant Secretary Taylor-Kale, let me start with you, and thank you very much for your comments. I want to commend you for the work you have been doing to develop our National Defense Industrial Strategy. It has been really a whole-of-Government effort, and I thank you for that.

One question I have, though, is—that concerns me, and I am seeing it across the board, is the decline of the defense workforce. Right? So there were 3 million people working U.S. defense industries in 1985. Today it is only about 1.1 million. And I—as we look to strengthen the Defense Industrial Base, that includes the workforce.

So can you talk a little bit about what we should be considering, what DoD is doing, how—what are we looking and what tools and resources are we utilizing to collaborate with Federal agencies, with the private sector, in strengthening that workforce.

Ms. TAYLOR-KALE. Thank you, ma'am. Glad you asked that question. Indeed, the decline of the defense workforce is a key area of

risk. It is a risk for production in general, certainly for production in defense critical supply chains. As part of the National Defense Industrial Strategy, we made workforce readiness one of the four strategic priorities for that very reason.

The Department of Defense is, in implementing this strategy and developing an implementation plan, workforce will remain a very important issue, and I would also like to note it is not just the Defense Industrial Base workforce but it is also the organic industrial base workforce, as well as our acquisitions workforce.

So we need all of them to be able to work in concert to be able to, again, bring the capabilities that our warfighters need at speed and at scale. We have a number of programs that we are developing. We have been focused on the submarine industrial base workforce.

I was just in Michigan on Monday with Secretary of the Navy Del Toro as we were unveiling a new initiative in Michigan to help reskill and upskill the workforce there, particularly automotive workers who may want to work in the submarine industrial base workforce, so creating an additional workforce in Michigan.

We continued to promote manufacturing and advance trade skills as well. Again, workforce remains a priority and will continue to be a priority for us as we continue to want to build out the resiliency of the industrial base.

Senator CORTEZ MASTO. I appreciate that. Thank you.

Let me jump to Assistant Secretary Rosen. I want to talk a little bit about CFIUS. I welcome your proposed rulemaking, which adds the Hawthorne Army Depot in Nevada to CFIUS. A couple of questions. I guess—I know you are adding 50 additional facilities as well. What factors contributed specifically to adding—if you can tell me, adding the Hawthorne Army Depot to the list?

Mr. ROSEN. Senator, thank you for the question and for your leadership on these issues. Of course, you mentioned Hawthorne, but there is a host of other facilities in your State that are on the list, importantly so, Nellis and others.

So back in—when Congress enacted FIRRMA, it gave us this new real estate jurisdiction. And, at the time, we worked closely with our colleagues at the Department of Defense to develop the initial list. And when we—when we came in, when I came in a couple of years ago, we looked at cases and we decided working closely with our colleagues at DoD to take another look. And, in 2023, we added eight additional bases, and as you point out, we are in the process of adding 59 more bases.

And I would defer to my colleague, Dr. Taylor-Kale, for some details on this. But as a general matter, what we look to is the sophistication of what's going on at these facilities, the possibility for potential espionage, how much of it is core national security, how much of it is training. That goes into whether something should be on a list and what the range should be.

And I should note that this update is the result of a broad strategic review led by my colleagues at the Department of Defense to really take a holistic view to make sure we are not leaving anything on the table in terms of plugging gaps to make sure the list is full and complete.

Senator CORTEZ MASTO. No. I appreciate that, and I—and you mentioned FIRRMA 2018, and I supported it, and obviously was looking at that as the security of our installations that you just mentioned in Nevada and throughout Nevada. So the collaboration is key, and it is nice to see that happening, so I thank you very much.

I only have so much time left. One final thing I just want to touch on, and, Assistant Secretary Kendler, you mentioned this, is more funds. More funds for the Department. My understanding is you haven't received funding—an increase since 2010.

And based on that, I would imagine it is challenging now, because of the increased capacity of your jurisdiction and oversight, to cover some of the coverage that you need with less resources. Is that one of the reasons why you are seeking an increasing? I guess talk a little bit about that, if you would.

Ms. KENDLER. Senator, thank you very much for the question. That is right. Taking inflation into account, our budget has essentially been flat for quite some time. Basically, the last decade it has barely kept up with inflation.

We do support the President's budget for fiscal year 2025, which is a downpayment on what we need in the Bureau of Industry and Security. If I had one ask, it would be for funds for IT modernization. We need roughly \$100 million to take antiquated systems and turn them into useful, productive data and analytic support.

We have had issues in providing answers to the Hill in a timely way because we don't have an updated modernization system, and we are not taking advantage of the data capabilities we have to the best of our ability.

With more funds, we would enhance our technical expertise, we would work on data and analytic capability, and then certainly our enforcement capacity as well.

Senator CORTEZ MASTO. Thank you.

Thank you, Mr. Chairman.

Chair BROWN. Thank you, Senator.

Senator Scott, the Ranking Member from South Carolina.

Senator SCOTT. Thank you, Mr. Chairman.

Ms. Kendler, I am glad you are here. My colleagues and I have written several letters calling for your testimony and on Commerce Department's firearm export licensing policies and regulations, because unfortunately your policies appear to have all the signs of political targeting, costing the industry an estimate \$500 million per year and generating no national security benefits.

Case in point is the company I mentioned during my opening testimony, M.G. Suber & Associates. I am looking at some of the denials on these licenses, and the recent, fascinating foreign policy pursuant to 22 CFR 120.18(a)(1) and (2) of the ITAR, the Department of State may deny a license or other approval when the Department deems such action to be in furtherance of world peace, denying a company the opportunity to sell firearms to Ecuadorian police.

Next one, same verbiage, deems such action necessary to further world peace, denying, again, another license to sell to the Ecuadorian military. This minority business owner is Ecuadorian, cares a lot about safety in a country where his mother born and raised,

Another one, furtherance of world peace. It is not only frustrating and exacerbating, but challenging to see this over and over and over and over again. Your firearm policy has resulted in over \$71 million in licenses canceled for this company, meaning they have lost their contracts, and they have lost the ability to support the police and the military across the Western hemisphere.

That does not mean that the Ecuadorian police did not find another channel. Of course, they went to Brazil, Czech Republic, and China to get these orders backfilled. You haven't prevented the sale of firearms. You have merely used a political tactic to harm an American business.

What is even worse is that it to me appears to be political targeting. The International Trade Association, under your leadership, has stopped this company but allowed competitors in some of our Nation's poorest areas to not be able to effectively create jobs, not be able to effectively produce a world-class competitive product and have a market to sell it to because you are trying to further world peace.

Thoughts?

Ms. KENDLER. Senator, I really appreciate you bringing up this topic, and I—

Senator SCOTT. I am not sure you do, but I think this is an important topic that reinforces this Administration's philosophical approach to trying to shut down or cutoff gun manufacturing in our own country.

Ms. KENDLER. I do appreciate you bringing it up, because I think there is a lot of misunderstanding about what we are trying to accomplish and what our rules have actually done. Our focus is on protecting national security. Full stop. We tailored the rule. Our presumption of denial in this rule is tailored to ensure that U.S. lawfully exported firearms don't end up in the hands of criminals, gangs, cartels, or terrorists.

Senator SCOTT. May I ask you a question there? Is there evidence that his company's firearms sold to the military and to the police have not been received by the military or police? Is there—is there something specific about this transaction or the other three that were denied?

Ms. KENDLER. Senator, I am not in a position to speak to a specific company's situation, but I certainly feel sorry for your constituent, and I would like to follow up with you in an environment where we can talk about a specific company. But let me be clear: our presumption of denial, it only applies to non-Government entities in the 36 countries designated by State as high risk.

So if these transactions are with Government entities, that is not the subject of our presumption of denial.

Senator SCOTT. Thank you. Let me just say, I think words mean things—Ecuadorian police, Ecuadorian police, Ecuadorian military, Colombian military.

Chair BROWN. Thank you, Senator Scott.

Secretary Taylor-Kale, the current DPA reauthorization expires next year, as you know. Senator Ranking Member Scott and I filed an NDAA amendment that would extend the DPA. Describe if you would why it is a critical tool that needs to be reauthorized and how DoD uses its authorities.

Ms. TAYLOR-KALE. Thank you, sir. Again, as you noted, DPA reauthorization is a priority for the Department of Defense. We use the DPA—all three titles—daily. A lapse would ultimately impact our warfighter needs and the ability of our—particularly our industrial base to address some of the long lead items, the long lead times, for critical defense components, and would ultimately, again, impact our warfighter.

You know, annually, we use Title I over 300,000 times to prioritize and allocate some of these urgent defense critical components and resolve supply chain issues. Without reauthorization, by next year we wouldn't be able to do that. We also, you know, use Title I really at no cost to the taxpayer.

A lapse would impact our prioritizations not just for us but also with our allies and partners. We have over 20 security supply arrangements with key partners and allies across the globe. Those security supply arrangements have been used with Israel, they have been used for Ukraine.

With Title III, it would also impact industry. It would impact small businesses. Forty percent of our Title III DPA awards go to small businesses and nontraditional defense suppliers. We are using the Defense Production Act Title III to expand and bring more nontraditional companies into the defense ecosystem. Without Title III awards in the—in the reauthorization of DPA title in general, we wouldn't be able to do that very important work.

Chair BROWN. Thank you. Secretary Rosen, 2018 Congress gave CFIUS the authority to require mandatory filings of foreign investments in critical technologies, as you know, since, and we have seen increasing attempts by malign actors to target U.S. critical infrastructure. That is why I am pushing to give CFIUS the ability to require mandatory filings. We need to know about these investments. It should not be optional. We file an amendment to NDAA to do this.

Would CFIUS—talk through whether CFIUS would be able to better protect the U.S. from dangerous foreign investment if it had the ability to require these mandatory filings for transactions related to infrastructure.

Mr. ROSEN. Senator, Chairman, thank you for that question and for your leadership on these issues throughout. You bring up critical infrastructure. It is a core component of what FIRRMA was all about. It is also a core component of what CFIUS reviews and looks at on a regular basis.

It is true that certain filings of critical infrastructure investments are mandatory, and I think the more, as a general matter, we want to make sure that we are seeing investments into places like critical infrastructure that raise national security risk.

I think the challenge is figuring out, how do you do that in a way that mandatorily requires what we need to see, what we want to see, but sort of weeds out some of the broader noise. And I think there is ways that we can do that through regulations and otherwise. And so we are committed to working with you on that effort, and we appreciate you spearheading that.

Chair BROWN. Thank you. Secretary Harris, the Administration has taken steps to establish a targeted program to ensure outbound U.S. investment doesn't strengthen China's ability to develop cer-

tain critical technologies. Describe—and, as you know, Senators Casey and Cornyn have led a bipartisan effort to codify an outbound investment program. Why—talk to us about the—talk to us, if you would describe why the Administration has taken a sector-based approach in its outbound investment program.

Mr. HARRIS. Thank you, Chairman, for that question. We are trying to take a very deliberate and narrow and tailored approach to address the national security risk, and that is certain outbound investments supporting the development of certain sensitive technologies in a country of concern. That is U.S. venture capital or private equity supporting the development of, say, sensitive semiconductor technology or AI-related applications in a Chinese startup.

We have been consulting very broadly with hundreds of stakeholders throughout the development of this program, and our belief is that with this sectorial approach, as we define it, it can be most administrable and most impactful, but also most narrow. Our goal here is to address that tailored threat while minimizing broader unintended impacts.

Chair BROWN. Thank you. Senator Van Hollen is recognized from Maryland. Are you ready?

Senator VAN HOLLEN. Thank you, Mr. Chairman. I appreciate it. We have an Appropriations Subcommittee hearing markup going on.

Thank all of you for what you are doing, both to strengthen our economy but also protect our national security at the same time. And I do want to just pick up on a couple of the questions that the Chairman asked, first with regard to the outbound investment screening.

And I applaud the Administration's leadership on this issue, working with our G7 partners and trying to design this in a way that you just said, Mr. Harris, was well tailored. I returned from a trip last week to a number of countries, including Saudi Arabia and UAE. There is a voracious appetite for U.S. technology, especially in AI, but also other sectors.

But if we are going to be successful in terms of targeted outbound investment screening, starting with the notification provisions, we obviously need our allies who are also in strong positions to, you know, provide investment in technology to cooperate fully. Right? Otherwise, we can shut the front door of the barn but leave the back one open.

Can you talk about the progress we are making getting some of our partners, whether it is the EU or other—others in East Asia, Japan, South Korea, to adopt similar measures with respect to outbound investment?

Mr. HARRIS. Thank you for that question, Senator, and I will quickly pull in Assistant Secretary Rosen as well for Treasury's role in leading the program.

I would say from a Commerce perspective, though, we have been with Treasury and the State Department very focused on working with allies and partners. We are in a situation where we have identified the threat, and we need to take action, and we are doing so. But we want this to be as inclusive and as broad as possible and have as many partners and allies share our perspective and take their own actions.

Senator VAN HOLLEN. I appreciate that. No. I was going to ask you, Mr. Rosen, as well. I know this is your portfolio at Treasury.

Mr. ROSEN. Thank you.

Senator VAN HOLLEN. If you could just speak specifically, not to the goals of enlisting support from our allies, but whether we are making substantial progress on that front and what more needs to be done.

Mr. ROSEN. Senator, you have hit the nail on the head in terms of the—sort of the backfill thing that we are focused on. I would say we are making progress. We are engaged, and we are committed to continuing that engagement.

I do think that a number of allies and partners are studying the issue to assess whether within their own economies they are similarly worried about the export of their dollars, of their—and their know-how in the same way we are. So I think we are getting different responses as a result, but I am encouraged by some of the statements that you alluded to, and it is an effort we are not going to give up on.

Senator VAN HOLLEN. I appreciate it. I just think we need to really, really push here. Otherwise, we will be in some ways putting restrictions, handcuffs, on our own company's investment when others are free to do so.

Under the jurisdiction of the Department of Commerce, Ms. Kendler, and specifically related to some of the machines that are used to manufacture very high-end chips for semiconductors, the United States has been very clear that we want to provide what we call the small garden, our crown jewels, but high walls. This also requires our partner's engagement.

So, for example, when it comes to some of the machines to help manufacture high-end semiconductors, we have worked with ASML and Tokyo Electron, but, you know, my understanding is that there may not be the progress that we had anticipated earlier.

So my question to you is, when and if would the United States want to apply the foreign direct product rule in order to ensure compliance with our goals? I don't know which of the two of—OK.

Ms. KENDLER. I will take that, Senator. Thank you.

Senator VAN HOLLEN. Thank you.

Ms. KENDLER. From the view of industry and security at the Commerce Department, multilateral coordination is crucial to export controls. Full stop. We are constantly building export control coalitions around the world on different critical and emerging technologies, like semiconductors.

The Dutch and the Japanese, as you alluded to, they impose their independent controls on semiconductor manufacturing tools. They are comparable to ours that—what we picked up last October in our amended controls. And that is a critical part of our work, ensuring that our allies and partners writ large understand the threat, that they understand what it means if we don't have controls in place, that it is fundamental to the coalition we built to respond to Russia's invasion of Ukraine.

It is a fundamental of how we are approaching quantum and other issues, as I alluded to in my opening statement. It is critical to us to keep that going.

Senator VAN HOLLEN. If you could—I asked specifically when and if we would apply the foreign direct product rule, which is obviously an escalatory measure, but one that may help get people’s attention to secure their cooperation. Can you speak to that?

Ms. KENDLER. We have increasingly applied the foreign direct product rule, which captures certain foreign-produced equipment under our regulations. We have increasingly used that as a tool. It is a heavy measure. Happy to talk to you about when and what circumstances might be appropriate.

Senator VAN HOLLEN. I would appreciate following up on that. Thank you, Mr. Chairman.

Chair BROWN. Thanks for those. Senator Kennedy of Louisiana is recognized.

Senator KENNEDY. Thank you, Mr. Chairman. Mr. Rosen—and thanks to all of you for being here. Mr. Rosen, Nvidia makes probably the most advanced artificial intelligence chips, does it not?

Mr. ROSEN. Nvidia does produce advanced chips, yes, Senator.

Senator KENNEDY. And those chips are highly coveted, because they can perform the massive computations needed to train AI systems; don’t they?

Mr. ROSEN. I believe so. Yes, Senator.

Senator KENNEDY. Yeah. And we have export controls on those chips; do we not?

Mr. ROSEN. We do, and that is a process led by my colleague, Ms. Kendler.

Senator KENNEDY. And we prohibit those chips from being sold to China; is that correct?

Mr. ROSEN. I don’t know exactly what chips are prohibited. I am going to defer to Ms. Kendler, but I know there are controls on the export of—

Senator KENNEDY. You don’t know whether the advanced Nvidia artificial intelligence chips are prohibited from being sold to China?

Mr. ROSEN. So, Senator, my understanding is that they are, but that is export controls. It lies with my colleague at the Department of Commerce.

Senator KENNEDY. OK. So how come we are selling them, we are allowing them to be sold to China?

Mr. ROSEN. Senator, I would respectfully defer. I don’t—I don’t oversee export controls. I oversee inbound investment into the United States.

Senator KENNEDY. Well, you control investment security; don’t you?

Mr. ROSEN. I do. And as—

Senator KENNEDY. All right. Let me ask Ms. Kendler. How come we are—how come we are being—we are allowing them to be sold to China?

Ms. KENDLER. Senator, our advanced computing controls from last October and the October before, they are absolutely targeted at the most advanced chips as you noted. We are controlling them for export to China, and we look, together with Departments of Defense, Energy, and State, at where they are going.

Senator KENNEDY. Yes, ma’am. But if you go on the internet, you will find 70 distributors, not seven, 70 distributors, which will sell Nvidia’s supposedly restricted chips to China. And, in fact, some of

them will sell to China the entire servers. They cost about \$300,000 apiece. They have got eight chips in them. Isn't that a fact?

Ms. KENDLER. Senator, I am not familiar with the website that you are referring to. But what I can tell you—

Senator KENNEDY. I am referring to 70. Do you read *The Wall Street Journal*?

Ms. KENDLER. On occasion, yes.

Senator KENNEDY. You should read this article. They have identified at least 70 distributors, and they have confirmed that these chips are being sold to China.

Ms. KENDLER. Senator—

Senator KENNEDY. And, I mean, this is very disturbing. One estimate, not according to the Center for a New American Security, it estimates that the median number of A-1 chips being sold already to China at 12,500. Isn't that correct?

Ms. KENDLER. Senator, any diversion of our controls would be a matter for export enforcement, and we are tracking that very closely.

Senator KENNEDY. But you are not aware that 12,500 have been sold?

Ms. KENDLER. Senator, we track all sorts of data through our analytic capabilities to understand illicit procurement networks. That is very important to our work.

Senator KENNEDY. But you don't—

Ms. KENDLER. It is something we are cracking down on.

Senator KENNEDY. —know about this 12,500?

Ms. KENDLER. I can't speak to the specific report that you are referring to, sir.

Senator KENNEDY. Well, you need to read the paper. No disrespect. These chips have been sold—and it has been confirmed—to China's most elite universities. They have been sold to the State research powerhouse, Chinese Academy of Science; haven't they? You don't know—do you know anything about that?

Ms. KENDLER. Senator, we look at license applications and determine whether they are consistent with national security. If it is not consistent with national security, we do not approve it.

Senator KENNEDY. Well, all you have got to do is go on—get your computer out and go on Google and search, and you will find 70 distributors that are selling these restricted chips that you are not shutting down. And *The Wall Street Journal* has confirmed all of this.

Ms. KENDLER. Sir, we would add entities like that to our entity list as a regulatory action. We would also—

Senator KENNEDY. But you haven't done it yet.

Ms. KENDLER. We would also have our enforcement colleagues investigate these kinds of allegations.

Senator KENNEDY. Were you aware of this before I raised it today?

Ms. KENDLER. Senator, I certainly am aware that when our laws are effective, illicit procurements networks stand up to—

Senator KENNEDY. Were you aware of these—

Ms. KENDLER. —violate them.

Senator KENNEDY. —70 distributors and the thousands and thousands that have been sold right there on the internet in front of God and country, bigger than Dallas? Was your agency in charge of enforcing this aware of that?

Ms. KENDLER. Senator, I would be happy to connect you with our enforcement team to talk about this in more detail.

Senator KENNEDY. Do you talk to your enforcement team?

Ms. KENDLER. Yes, sir.

Senator KENNEDY. I mean, who is on first? What is on second? We have got export controls here, and all you have got to do is go on the internet and China buys them.

Ms. KENDLER. The export—

Senator KENNEDY. Are you aware—let me—were you aware of this before I raised it today?

Chair BROWN. Senator Kennedy, you have made your point clear. I share your concerns. I think this is one reason why BIS needs more funds.

Senator Smith from Minnesota is recognized.

Senator KENNEDY. Well, I—can I just say one more point?

Chair BROWN. You certainly may.

Senator KENNEDY. I don't think they need more money.

Chair BROWN. Well—

Senator KENNEDY. I think they need people that talk to each other and know how to use an internet and know how to read articles in *The Wall Street Journal*. This is not—you don't have to be an astrophysicist here.

Chair BROWN. Senator Smith.

Senator SMITH. Thank you, Chair Brown, and thanks to all of you for being here. I really appreciate it.

I would like to direct my first question to Assistant Secretary Taylor-Kale, if I may. The recent disastrous CrowdStrike incident I think exposed the alarming vulnerabilities that can result when too many critical systems and capabilities are dependent on a single source component, and that faulty software update crash—it apparently crashed over 8 million Windows devices, and airlines were crippled, banking systems, hospitals. It was a mess. A lot of people paid the price for that.

My question is, the DoD's industrial base strategy includes efforts to reduce the risks associated with overdependence on a single or potentially adversarial source for national critical capabilities. I am wondering, how is the DoD thinking about the national security risks that can stem from instances like the CrowdStrike outage where there is vulnerability from a single source product that can crash critical systems?

Ms. TAYLOR-KALE. Ma'am, thank you for that question. Single sources of—in our supply chains, and particularly our defense critical supply chains, remains a huge and incredible risk for our industrial base, and for the Department of Defense in general, for us being able to provide our warfighters with the capabilities that they need at speed and at scale.

An issue like the one that you raise with CrowdStrike is one that obviously we all experienced. I experienced it myself personally on Monday trying to leave Michigan. But, in general, we address sort of our supply chain issues, you know, looking at—broadly looking

across the board. We also, through our Chief Information Officer, look at cyberthreats in particular.

And I want to emphasize the importance of cyber as part of the sources of risk to our industrial base, particularly to manufacturers, as well as part of the umbrella of the National Defense Industrial Strategy. CIO also issued the cyber—the DoD Defense Individual Base Cyber Strategy as well.

So we continue to look very closely at these and look at ways in which they affect particularly the Defense Industrial Base and how we can intervene.

Senator SMITH. Thank you. I appreciate your response. I think it was just sort of impossible for most Americans to believe that everything could just be so screwed up because of one software update gone awry. And I think when you think about what that might mean for other, you know, highly important systems that we rely on for so many other things, it is really concerning.

I want to ask you another question. This one has to do with drug onshoring. So the FDA tells us that nearly 70 percent of the ingredients that—the ingredients in medications that Americans take are sourced overseas, mostly India and China, and the finished drug supply is already heavily reliant on overseas supply chains, again, mostly from India and China.

So could you talk about what the risks are that are posed by this reliance on foreign manufactured drugs, especially medications like antibiotics, what impact that has on military readiness and civilian health? And what tools does the Department of Defense have to promote domestic manufacturing of these critical medical products?

Ms. TAYLOR-KALE. Ma'am, I want to underline the concerns that you raise, particularly with pharmaceuticals and the effect that they have on our supply chains and ultimately to our warfighters. I don't, in my purview, handle these issues within the Department of Defense, but I also want to note that Mr. Harris also does within the Commerce Department. He may have something to add to this.

Senator SMITH. Thank you. Mr. Harris.

Mr. HARRIS. Thank you, Senator. We absolutely share your concern that we need to be focused on where there are dependencies, where there are single sources of supply, and we have an urgent need to be more proactive and strategic in our approach to supply chains. We all collectively learned lessons in the pandemic, but it is not just about where the market might not function or where the supply might be—

Senator SMITH. Right.

Mr. HARRIS. —too brittle of a supply chain. There are also national and economic security risks in these supply chains. You noted a perfect example. Americans expect every day that they would have what they need in the medicine cabinet or on the kitchen table, and the supply chains are what gets those products to point.

My team in the Commerce Department and in the new supply chain center that we have created, we have been working with the Health and Human Services Agency and others to try to assess the data and identify what is of greatest concern and who do we need to work with to try to improve resiliency in that supply chain.

Senator SMITH. Thank you. Thank you very much.

Mr. Chair, I would just note that I have two bipartisan bills to address this issue, one with Senator Cassidy, which would provide fundings to antibiotics manufacturers to bring those factories back to the United States, and the second with Senator Cotton would provide incentives to drug manufacturers to produce finished drugs here in the United States by providing higher reimbursement for those products.

I look forward to working on those proposals with any of my colleagues who are interested.

Chair BROWN. Thank you, Senator Smith.

Senator Britt from Alabama is recognized.

Senator BRITT. Thank you, Chairman, and thank each of you for being here today. We appreciate it.

Look, we all know the ever-growing threat that is posed by the Chinese Communist Party, and whether the CCP—no matter what they are doing, undermining the American worker, stealing intellectual property, buying up our farmland, they have demonstrated a disregard for international rules.

So when we are looking at that, it seriously doesn't matter if it is trade, if it is intellectual property, anything standing in their way, they are willing to just bulldoze straight through that. And American companies across every single sector of our economy are under pressure as a result.

So I am looking at AI, computing, energy, robotics, just influence or attempts to influence our institutions, the buying up of farmland. We could go on and on and on. The Chinese Communist Party is going to stop at nothing until they achieve their ultimate goal and they upend international order.

So using the tools at our disposal, whether it is export controls, CFIUS, or sanctions, we must pursue a strategy that strikes the right balance between protecting U.S. industry and businesses and hardworking Americans from the threats that are imposed by the Chinese Communist Party and other adversaries, while also allowing our economy and capital markets to thrive and to remain dominant.

On this, a recent New York Fed report raised questions about the effect of unilateral export control policies. The report highlights the unintended consequences, like lost revenue to U.S. firms, loss of start market capitalization for U.S. companies, and, worse yet, unintentionally propelling Chinese firms to innovate and develop and advance technologies in-house. In that end, the American consumer is the one that pays the price, and that is who I am concerned about.

Ms. Kendler, how do you think we strike the balance between cutting off China's access to our critical technologies while also ensuring American consumers don't pay the ultimate price?

Ms. KENDLER. Thank you, Senator. This is a question that we struggle with every day. Our focus is on maintaining national security. That comes before all.

Senator BRITT. Good.

Ms. KENDLER. But part of national security is U.S. technological leadership. And so I think the first thing I would point you to is the multilateral approach to export controls and the calibrated approach to export controls. So such as in our semiconductor controls

where we have targeted the most advanced chips, we are not trying to unduly interfere with business that doesn't cause a national security risk. We are trying to target our controls and create them in a way, together with our interagency partners, that attacks the most important need.

The danger of not using multilateral controls is that we may fail. We are damming half the river, if it is only the United States imposing controls and not our partners and allies or other supply countries. We are also potentially incentivizing foreign companies to design out U.S. components as they manufacture goods. So this is something we pay a great deal of attention to as we don't take our eye off the national security ball.

Senator BRITT. Well, and in that vein, unfortunately, since it was reauthorized last—in 2018, the Defense Production Act has become increasingly used. You have seen President Biden and Vice President Harris again acting out of the bounds of Congressional intent, this time using it to further the Green New Deal agenda and by boasting productions of things like solar panel parts.

Using the Defense Production Act for partisan priorities that have little to do with national security undermines the critical use of that tool and the way that it was intended to essentially give our Nation the ability to defend ourselves and our allies.

We are considering reauthorization ahead of 2025, and we need to ensure that it is actually being appropriately utilized. And so, Ms. Taylor-Kale, I understand you recently released the first National Defense Industrial Strategy. Can you share with us the status of implementation? And, more broadly, what is the state of the industrial base and ensuring that our warfighters are properly equipped?

Ms. TAYLOR-KALE. Thank you, ma'am. I want to emphasize again that the Department of Defense strongly supports the reauthorization of the Defense Production Act. The Defense we use the Defense Production Act daily, all three titles, to make sure that our supply chains, our defense critical supply chains, are secure.

Last year, fiscal year 2023 alone, we invested \$733 million in critical minerals, microelectronics, and other areas where there are gaps in our supply chains. We very strongly see the importance of this with respect to some of the investments that you mentioned. I can, again, only speak to Department of Defense investments that I oversee, and I refer you to other agencies and particularly Department of Energy or HHS.

Senator BRITT. Right. But the warfighters specifically.

Ms. TAYLOR-KALE. And that is how we use the Defense Production Act within the Department of Defense. Again, it is to address long lead times of critical materials, for instance, materials that go into rare earth elements, that go into the F-35 for instance. We use the Defense Production Act daily to support the warfighter.

Senator BRITT. Thank you.

Chair BROWN. Senator Warnock of Georgia is recognized.

Senator WARNOCK. Thank you so very much, Chair Brown.

I don't believe that giant American corporations should get richer by selling their technologies to authoritarian regimes or human rights abusers. And that is why I was glad to see the Biden-Harris administration take steps in 2021 to further center human rights

in U.S. foreign policy through the Export Controls and Human Rights Initiative, an effort aimed at curbing the misuse of American technology by repressive Governments and regimes whose human rights record we rightly deplore.

Twenty-five Nations have signed on to the initiative's code of conduct leading to more of our allies considering human rights when reviewing their exports of technologies that can perpetuate human rights abuses. We don't want to make the trampling of human rights efficient.

Ms. Kendler, can you highlight some successes from the Export Controls and Human Rights Initiative and how they contribute to efforts to combat authoritarian regimes?

Ms. KENDLER. Senator, thank you for this question. Human rights are front and center in how we consider export controls. The ECHRI, as we know it, the Export Controls and Human Rights Initiative, has been very helpful in bringing together countries that share values, even when they don't have export control systems of their own. And it has enabled a dialog that is desperately needed for our national security and foreign policy.

Just today, the Commerce Department released a proposed rule that is connected to ECHRI. We are looking at foreign security end users in countries of concern, authoritarian countries like you note, to ensure that U.S. persons are not supporting jail operators, foreign police, and that sort of thing. And that is a proposed rule. We are seeking industry comment, but it is connected to ECHRI in the sense that it moves our human rights protections forward.

We have also been very active at the Commerce Department in adding entities to our entity list requiring specific licenses for companies and other organizations that may be involved in human rights abuses, contrary to U.S. national security and foreign policy.

Senator WARNOCK. So it is important in terms of the advancing of our own values and our commitment to human rights. But could you say more about why it is important that the United States of America lead in this space. My sense and core belief is that there is no replacement for American leadership in the world. It is indispensable. And can you say more about the geopolitical implications of us leading in this space?

Ms. KENDLER. U.S. technology is the best in the world. We need to take a leadership role to ensure that it is not used in a way that is contrary to our values. And by taking that stance and working with our allies through multilateral regimes, plurilateral regimes, bilateral relationships, we can bring others into that fold.

And there are many countries around the world who do share our values and who are looking at things like facial recognition systems and saying that may be appropriate in an—I don't know, an airport context. It is not appropriate when you are surveilling minority populations in Xinjiang or Tibet.

Senator WARNOCK. So you would say that the United States is uniquely positioned to lead in this space. And would you also say that it has national security implications for us?

Ms. KENDLER. Yes, Senator, I would.

Senator WARNOCK. Are additional Congressional authorities necessary to expand and improve the efficacy of these initiatives?

Ms. KENDLER. Senator, there are several ways where we could bring in technical expertise into the Bureau of Industry and Security. One thing that comes to mind is a highly qualified experts program that we are seeking authority for.

We could bring in experts on a temporary basis into the Bureau of Industry and Security who know these technologies well. That is an area where we welcome an opportunity to obtain additional authorization and resources.

We would also look at some provisions in our regulations like remote access and the opportunity to control access to data centers and other high-end advanced technology. That is an area where expansion of our authorities under ECHRI would be helpful.

Senator WARNOCK. Well, thank you so much. There are more questions that I could ask, but maybe we can follow up later. But I am grateful that the Biden-Harris administration understands that export controls can be an effective tool to combat authoritarian regimes. This is important in this moment especially when you look at the geopolitical situation, the effort by some to advance a kind of authoritarian approach both internationally and I would say domestically.

So thank you for your work. As surveillance technology continues to improve, we must ensure American corporations are not making money from authoritarian regimes and human rights abusers. All of us have a stake in that project.

Thank you very much.

Chair BROWN. Thank you, Senator Warnock. Senator Warren from Massachusetts is recognized.

Senator WARREN. Thank you. Thank you, Mr. Chairman.

So the Committee on Foreign Investment in the United States, or CFIUS, reviews foreign investments in our country to make sure they don't pose risk to national security. Increasingly, foreign companies are building crypto mining facilities on U.S. soil. These mines are actually warehouses stuffed with computers that process crypto transactions and produce new crypto tokens.

They are loud, they are hot, and they suck up a ton of electricity, which can crash the power grid. And that is why many countries have banned crypto mining, leading more foreign companies to set up shop here in the United States.

According to a blockchain analytics firm, today one third of crypto mining facilities in the U.S. are owned by citizens of the People's Republic of China, including people with direct ties to the Chinese Government. Now, crypto mining is a disaster for the environment, and it can pose national security risks as well.

In May, at CFIUS's recommendation, President Biden issued an order requiring the Chinese national owners of a crypto mining facility in Wyoming called MineOne, to divest their ownership and remove the crypto mining equipment from the premises.

Assistant Secretary Rosen, you are the head of CFIUS, so you oversaw the investigation into MineOne and told the President that the divestment was essential. The divestment order cited two primary factors. One, the technology inside MineOne could be used for surveillance; and, two, MineOne was located one mile from a strategic missile base housing intercontinental ballistic missiles.

So I want to ask you, could the equipment inside that crypto mine have been used to spy on our military operations and our nuclear weapons system?

Mr. ROSEN. Senator, thank you for the question, and I think pointing out this case in particular, I am limited in terms of what I can say about this particular transaction. But to answer your question, there is a generalized concern that sophisticated equipment in proximity to sensitive facilities can be used for espionage.

Senator WARREN. OK. So can be used for espionage. Foreign adversaries are using crypto mines to spy on U.S. military operations. That is an obvious national security risk, but it isn't the only risk. Foreign-owned crypto mines also threaten our energy grid.

According to an analysis by *The New York Times*, bitcoin mines in U.S. owned by Chinese nationals use enough energy to power 1.5 million homes. National security experts have warned that foreign-owned crypto mining facilities' connection to our energy grid could leave the U.S. vulnerable to targeted blackouts and cyberattacks.

Assistant Secretary Rosen, if China or another foreign country had the power to crash a significant portion of our country's power infrastructure, could that threaten our national security?

Mr. ROSEN. Senator, of course an impact on our energy sector, our energy resources, our energy supply chain, could very much have a national security impact.

Senator WARREN. All right. There is yet another risk as well. Foreign nationals have been able to buy up crypto mines in the United States in secret. How? By paying in crypto. Crypto allows them to bypass our traditional banking system and the anti-money laundering rules that are supposed to prevent any anonymous foreign money from coming into the United States.

In fact, that is exactly how a Chinese investor was able to secretly buy a \$6 million crypto mine in Texas. It is also how U.S.-based crypto mines have been able to secretly send millions of dollars back to China.

Assistant Secretary Rosen, do you agree that we need to plug the holes in our anti-money laundering rules that have allowed foreign nationals to secretly buy U.S. crypto mining facilities or make other kinds of investments in the U.S. without our knowing about it?

Mr. ROSEN. Senator, I certainly share your concern about ultimate beneficial ownership and making sure that we know who is doing the buying. I can speak for the CFIUS context. When we look at a transaction or try to find a transaction, that is a critical component to our diligence.

Senator WARREN. All right. Crypto mines could be used by our adversaries to spy on our military bases or to bring down our power grid or to move money in and out of the country in secret. Last year, the Treasury Department requested additional tools from Congress to prevent China, Iran, Russia, and other foreign countries from using crypto to evade sanctions and launder dirty money. It is time for us to pass the laws that Treasury needs.

Thank you, Mr. Chairman.

Chair BROWN. Thank you, Senator Warren.

Not unrelated to our comments yesterday, I introduced the CAR Act to be proactive and stay ahead of the threat that China—Chi-

nese connected vehicles pose to our national security and to American privacy—to Americans' privacy, another threat that we have the chance to meet now early before it—before there are more Chinese connected vehicles on our streets.

Ms. Kendler, I hope you and your colleagues will work with me on that effort.

Thank you to the witnesses today.

For Senators who wish to submit questions for the record, those questions are due 1 week from today, Thursday, August 1.

To the witnesses, you have 40 days to—45 days to respond to any questions.

Thank you again. The Committee is adjourned.

[Whereupon, at 11:30 a.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

PREPARED STATEMENT OF CHAIR SHERROD BROWN

We face an uncertain world with many geopolitical challenges—from Russia’s continued brutal invasion of Ukraine, to ongoing conflicts in the Middle East, to an increasingly aggressive and capable Chinese military.

And we know that China has built that military capability with the help of American corporations, and even American tax dollars.

For too long, our Government was willfully blind to the threat China posed. Multinational corporations eager to move jobs wherever they could pay ever-lower wages, lobbied for permanent normal trade relations with China.

And when corporations moved production overseas, they outsourced the technology and trade secrets along with it. We did nothing to stop it, and now we’re paying the price.

We cannot make the kinds of mistakes we have in the past. We have to be proactive about these threats, and take action now to protect our national and economic security. And we need to be clear—those two issues are intimately connected. You can’t separate the economy and our national security.

Today, hostile Governments are working together more and more to challenge the interests, security, and values of the United States, and our allies and partners around the world.

Increasingly, hostile Governments use our own technology to fuel their destructive efforts.

We must lead efforts to stop it.

It is the U.S. Government’s job to police the flow of sensitive and so-called “dual use technologies”—technologies that can be used for both military and civilian purposes. The Departments of Commerce and Treasury—along with DOD, State, and other agencies—try to restrict the flow of sensitive technologies to our adversaries.

We cannot allow U.S. innovation and investments to be used against us.

Against that backdrop, NATO met earlier this month and issued a statement addressing these threats.

Specifically, NATO leaders called on China to “cease all material and political support to Russia’s war effort” including “the transfer of dual-use materials, such as weapons components, equipment, and raw materials that serve as inputs for Russia’s defense sector.”

That followed last month’s G7 Summit in Italy, where the United States and our allies reaffirmed our shared efforts to “implement export controls to address risks to international security” and “ensure the effectiveness of our respective foreign investment screening.”

The G7 leaders also noted that “measures designed to address risks from outbound investments could be important to complement existing tools of targeted controls on exports and inbound investments.”

A core element of this Committee’s work has been to establish and conduct oversight over our export controls, investment security, and Defense Production Act authorities.

The Treasury and Commerce Departments have had active and growing caseloads since our hearing last year.

They have expanded controls on semiconductors, equipment, and services that could support China’s semiconductor ecosystem.

They have taken steps to establish an outbound investment program that would enable us to better understand—and stop—U.S. investments that build up China’s military.

And they have recently issued a proposed rule that would significantly expand the Committee on Foreign Investment in the U.S.’s ability to review foreign real estate investments near military bases, like Wright-Patterson in Dayton.

This is the kind of action that I and many from both parties have been pressing for. I hear from farmers in Ohio near our military installations who are very concerned about this.

As we use our export control and investment security policies to restrict China’s ability to use U.S. technology and investments to advance their military capabilities and human rights abuses, we also must bolster our own domestic capabilities.

To that end, I was pleased to see Dr. Taylor-Kale and her colleagues release the Defense Department’s first ever National Defense Industrial Strategy earlier this year.

As a critical economic security tool, this Committee has jurisdiction over the Defense Production Act, which must play a vital role in advancing that strategy.

In Ohio, we know the potential here to harness the talents and patriotism of American workers to protect our country.

For decades, the Air Force Research Lab at Wright-Patterson Air Force Base in Dayton has been the home of the DPA Title III program.

Aside from the good work being done at AFRL, the Defense Production Act gives the Administration the authority to allocate and prioritize critical materials and to increase domestic productive capacity to address industrial shortfalls.

In other words, the DPA allows the Defense Department and other agencies to invest in American manufacturing that can support U.S. national security, as well as making us more prepared for emergencies.

This work could not be more urgent.

For decades, corporate offshoring and consolidation and restructuring—really just another elite business-school term for finding new ways to screw workers to increase profits—all weakened our domestic manufacturing sector.

Ohioans know what that has done to our towns, our families, our economy. And increasingly, people in this town are finally waking up to how it's weakened our national security.

We know that when companies outsource jobs, they outsource technological capabilities along with them.

There has not been enough appreciation for how much innovation happens on the production floor, by workers.

Over the past few years, we have finally taken steps to reverse that course—passing the CHIPS and Science Act and the Bipartisan Infrastructure Law.

And we have increased funding for strategic investments using the Defense Production Act.

But we must do more.

As Congress prepares to reauthorize the Defense Production Act, we need to look at new ways the DPA can support American industrial capabilities and help us revitalize our domestic industrial base to meet current and future challenges.

Today we will also discuss how we are working with our partners to coordinate our export controls and investment security policies, and what steps Congress can take to strengthen these authorities.

We look forward to testimony from this panel of witnesses, who can update the Committee on their important work.

PREPARED STATEMENT OF SENATOR TIM SCOTT

Thank you, Mr. Chairman.

I would like to start by reminding this room and our witnesses of the important role they play in safeguarding our Nation's economic and national security priorities.

President Reagan once rightly noted that we are in “a different world, and our defenses must be based on recognition and awareness” to combat our enemies of the modern day.

While he was talking about the Soviets, unfortunately, many of our adversaries remain the same.

Russia, China, Iran, and North Korea.

But thankfully, what also remains the same is the American spirit to innovate and to create the world's leading technologies.

My home State of South Carolina is an excellent example.

From F-16s to the world's best luxury airliners to leading automotive manufacturing to creating next generation technologies—I'd say South Carolina is simply our future.

But to safeguard that future, we must ensure that policies created here in Washington don't cut off growth and stifle future innovation.

We must have a global economy where America is the leader.

After more than 3 years of President Biden's policies we have seen soaring inflation that is crushing everyday Americans, wars across our globe, and our enemies challenging us and our allies at every single turn. We can, and we must frankly, do better.

So today, as we discuss and evaluate some of our economic national security tools—our export controls, investment security, and the Defense Production Act, we must keep these principles in mind.

At times, we must be willing to reassess our policies and re-tool our positions.

And, frankly, let's consider our allies.

One thing we certainly learned through COVID, was depending on China is a really bad strategy.

To be effective in countering China, we must work with our allies so that China can't easily find work arounds to U.S. export controls, by simply buying these same technologies and equipment from our friends.

A failure to look holistically at our economic strategy can and will damage American security, competitiveness, and unfairly, leave U.S.-led industry behind.

In fact, a recent study by the New York Federal Reserve found that the Biden administration's export control policies on the semiconductor industry have led to decreased profitability, job losses, and \$130 billion in financial loss across the industry.

With new reports that these types of policies have directly led to thousands of layoffs in States ranging from Ohio to New York—we must scrutinize the actions leading to these results.

But it doesn't stop there.

In my home State of South Carolina, recent actions by the Commerce Department to revoke thousands of export licenses for gun manufacturers have resulted in millions of dollars in losses.

I've sent three letters to the Commerce Department on this issue. And now reports suggest that we will see over \$500 million in annual losses across U.S. firearms manufacturers.

Mr. Chairman, I have a letter here that I would like to submit for the record. In my home State of South Carolina, a small, minority-owned firearms business had more than \$71 million worth of export licenses revoked by the Biden Commerce Department.

Unfortunately, this meant that the firm defaulted on multiple international contracts.

And now those same contracts are being backfilled by China and others. And it's my understanding that these licenses were revoked for "foreign policy" reasons such as the "furtherance of world peace."

So instead of supporting American companies, we just handed over this marketplace to China.

Export controls, investment security, and important tools like the Defense Production Act, should be used in a responsible manner that maximizes growth here at home and economic pain for our adversaries.

I strongly believe that when we have a better domestic environment, a better ability to innovate and manufacture—that means that America is winning.

Thank you and I look forward to discussing these important issues with our witnesses.

PREPARED STATEMENT OF THEA KENDLER

ASSISTANT SECRETARY FOR EXPORT ADMINISTRATION, DEPARTMENT OF COMMERCE

JULY 25, 2024

Chairman Brown, Ranking Member Scott, distinguished Members of the Senate Banking Committee, thank you for inviting me to testify about the ongoing efforts of the Commerce Department, Bureau of Industry and Security's (BIS's) Export Administration to administer U.S. export controls to protect U.S. national security and foreign policy interests. We remain laser-focused on addressing the challenges posed by the People's Republic of China (PRC's) Government's military modernization and human rights abuses and the Russian Federation's (Russia's) efforts to obtain dual-use technologies to further its illegal, unjust, and unprovoked aggression against Ukraine. We have been navigating these immense challenges by reinvigorating our multilateral efforts and by employing export controls in new ways. Now more than ever, our work hinges on deep collaboration with allies and partners. We are also making every effort to ensure that BIS's Export Administration (EA) is positioned to successfully counter the national security challenges of the future, starting with those related to misuse of artificial intelligence (AI).

BIS is responsible, along with interagency partners, for protecting U.S. national security and foreign policy interests by ensuring that U.S. technology is not obtained by foreign countries and entities of concern to harm the United States. The bureau also works to promote American technological leadership. This responsibility stems from BIS's authorizing statute, the Export Control Reform Act of 2018 (ECRA), which describes the policy goals for BIS's administration and enforcement of its export control system. While I lead the regulatory and licensing functions of BIS, my colleague in Export Enforcement (EE), Assistant Secretary for Export Enforcement Matthew S. Axelrod, leads the bureau's law enforcement agents and analysts in the

exercise of administrative and criminal enforcement authorities for alleged violations of our export controls.

Through the Export Administration arm of BIS, which I lead, we identify sensitive U.S. technologies of national security and foreign policy concern, develop policies and strategies for protecting these technologies, and review license applications submitted by exporters to determine whether specific transactions are consistent with U.S. national security and foreign policy interests. We also analyze data, industry information, and classified reporting to assess the effectiveness of our controls, the availability of foreign technology (including identifying sensitive technologies developed by ally and partner countries), and foreign end users that require extra scrutiny before receiving U.S. technology. In administering U.S. export controls in close coordination with the Departments of State, Defense, and Energy, we endeavor to take a multilateral approach. To be sure, there are times where unilateral export controls are necessary, however, as ECRA notes, “[e]xport controls that are multilateral are most effective [. . .]”. Accordingly, coordinating with our allies and partners on export controls is a longstanding BIS priority.

In today’s testimony, I will discuss the long-standing controls we have in place for the PRC, enhanced controls adopted under the Biden-Harris administration, the targeting of PRC entities of concern, the efforts we have taken to support our closest allies and partners, and the need for increased funding to support our mission.

PRC Dual-Use Export Controls and Licensing

BIS maintains comprehensive controls on the exports of sophisticated technologies to the PRC. BIS also controls low level technologies to preclude exports to untrusted end users, PRC military activities, and weapons of mass destruction (WMD) programs. This includes the imposition of license requirements for:

- All military and spacecraft items under BIS jurisdiction (which are subject to a statutory policy of denial);
- All multilaterally controlled dual-use items;
- A large number of dual-use items with extensive commercial applications if the item is knowingly intended, entirely or in part, for a military end use or military end user in the PRC;
- All items under our jurisdiction if the item is exported knowing it will be used in certain WMD programs;
- All items under our jurisdiction if the item is exported knowing it is intended, entirely or in part, for military–intelligence end uses or end users in the PRC; and
- All items under our jurisdiction if the item is destined for a party on BIS’s Entity List.

In addition, BIS prohibits certain U.S. person activities that would support WMD-related activities or military-intelligence end use or end users in the PRC, even if no items subject to our jurisdiction are involved, absent authorization.

With our interagency partners, we review all of the license applications for the PRC to determine a risk of diversion to military end uses or end users, WMD end uses, or abuses of human rights. We evaluate license applications—taking into account open source and intelligence information—based on the technology at issue, the country at issue, the entity using the item, other parties involved in the transaction, and how the item will be used. One of the primary factors we consider is the risk of diversion of the technology from the transaction details articulated in the license application instead to a country, end user, or end use of concern. License applications are reviewed with a presumption of denial where there is evidence of a substantial risk of diversion.

As Secretary Raimondo has stated: “China today poses a set of growing challenges to our national security. It is deploying its military in ways that undermine the security of our allies and partners and the free flow of global trade” The Chinese Communist Party (CCP) under President Xi Jinping has set a goal to develop the People’s Liberation Army (PLA) into a “world class military” and overtake the United States and its allies and partners by dominating certain advancing technology sectors such as AI; autonomous systems; advanced computing, semiconductors and microelectronics; quantum information sciences; biotechnology; space systems; and advanced materials and manufacturing.

To fulfill this vision, the PRC Government is going to great lengths to obtain key advanced technologies with military potential. Export controls generally operate by trying to control military uses while allowing civilian uses of technology. The PRC Government’s military-civil fusion (MCF) strategy deliberately blurs lines between commercial sectors and the PRC’s defense industrial base. This strategy is even

more concerning where the PRC's Government structure gives leadership the power to coerce information and assistance from companies that have little choice but to comply. Accordingly, the goals of the PRC's MCF strategy, situated within the PRC's Government system, have necessitated stronger export controls by the U.S. that target predominantly commercial items that can be used in military applications.

In the face of the PRC's challenges to global peace and security, the United States and our allies and partners must safeguard our core technologies by continuously and proactively reviewing and updating our export control policies.

BIS has long restricted access by PRC entities to dual-use items of national security and foreign policy concern, including emerging technologies. Together with our interagency partners in the Defense Department's Defense Technology Security Administration, the Energy Department's National Nuclear Security Administration, and the State Department's Bureau of International Security and Nonproliferation, we work to address national security threats and foreign policy concerns posed by the PRC Government. These efforts include U.S. control list proposals to the appropriate multilateral export control regimes, amendments to the Export Administration Regulations (EAR), review of export license applications, and identifying specific end users of concern. Because each agency brings different considerations and understanding, BIS relies on the interagency for its varied perspectives to ensure decisions that best protect U.S. national security and foreign policy interests.

License applications submitted by exporters and reexporters to send items to the PRC receive close scrutiny by BIS and our interagency partners. In calendar year (CY) 2023, license applications for the PRC had an average processing time (APT) of approximately 92 days. This APT is significantly longer than the CY 2023 APT for non-PRC cases of approximately 31 days. Compared to CY 2021 APT for PRC cases of approximately 76 days, we see a 21 percent increase in just 2 years. As evidenced by this data, BIS with its interagency colleagues, is taking the time to ensure that PRC licenses are carefully reviewed. We prioritize comprehensive review of relevant open source and intelligence information over speed.

In CY 2023, licenses reviewed for the PRC comprised approximately 11 percent of all applications reviewed by BIS. For items, including commodities, software, and technology (including domestic technology transfers, known as deemed exports), BIS and our interagency partners reviewed approximately 4,494 export and reexport license applications. Of these, approximately 30 percent were denied or returned without action.

In general, statistics regarding the interagency licensing process must be considered in light of the inherent restraint exercised by U.S. companies that generally do not waste time or resources applying for licenses they know will be denied or subject to lengthy interagency review. U.S. exporters should, before filing license applications know the parties in their transactions, including intermediaries and the end user, as well as the end user's intended use of the item. Exporters who do not do this risk either a return of rejection or return without action of their license application. After reviewing BIS's extensive know-your-customer and red flags guidance, many U.S. exporters do not submit license applications for transactions they contemplate are likely to be rejected. In fact, applications for exports to the PRC dropped by 10.7 percent between CY 2022 and CY 2023 (although volumes are still higher than during the height of the pandemic).

BIS's approach to the PRC is calibrated and targeted. Using a scalpel approach, we seek to restrict the PRC's military modernization efforts by restricting key, sensitive technologies without undercutting U.S. technology leadership and unduly interfering with commercial trade that doesn't undermine our national security and foreign policy.

We remain focused on aggressively and appropriately using our tools to contend with the long-term strategic competition with the PRC. Since the last time I was before this Committee in May 2023, we have strengthened the U.S. dual-use export controls policy toward the PRC:

Artificial Intelligence Item Controls

- In October 2023,¹ we updated the advanced computing and the semiconductor manufacturing equipment rule, which was published in October 2022. A core component of imposing export controls is continually assessing their overall effectiveness and keeping pace with technological changes. The October 2023 update revised the control parameters for advanced integrated circuits, and broadened the destination-based controls to cover additional destinations of concern. We also imposed worldwide license requirements for certain advanced inte-

¹ <https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3355-2023-10-17-bis-press-release-acs-and-sme-rules-final-js/file>

grated circuits and related specified end-uses when done for entities headquartered in, or with an ultimate parent company headquartered in Macau or a destination subject to an arms embargo such as China.

- Many of the updates were done to address the PRC's vast and aggressive efforts to undercut our controls through sophisticated evasion and circumvention tactics. Our policy intent remained the same. We sought to target the PRC's ability to acquire or produce the most advanced chips with direct AI applications for the development of advanced weapons systems, malicious cyber activity, and other military and intelligence applications. At the same time, we sought to minimize unintended impact on trade flows and on the economies of our partners and allies.

U.S. Participation in International Standards Setting Bodies

- Last week, to ensure robust U.S. participation and leadership in international standard-setting bodies, we amended the EAR to ensure that export controls and associated compliance concerns do not continue to impede and jeopardize U.S. participation and leadership in legitimate standards-related activities. Certain export control-related factors in the standards-making process led to an environment of regulatory uncertainty and decreased participation of U.S. companies in critical standards-related activities. This decrease in participation is a national security concern as it not only limits U.S. leadership in standards development, but also leads to the PRC racing to replace U.S. participation with their own leadership and standards. This uncertainty contributes to the potential of a global standards environment that works in opposition to U.S. technological leadership and broader interests. The changes made by last week's rule help ensure that U.S. participation and leadership in the development of critical and emerging technology standards with our allies and partners remains strong.

In addition to its technology-based controls, BIS increasingly has used entity-specific restrictions, primarily through the Entity List, to restrict trade to actors of concern in the PRC. Through the interagency End User Review Committee (ERC), BIS and our interagency partners review PRC companies, both State-owned and commercial, to determine if they are reliable recipients of U.S. technology.

Currently, we have over 800 PRC parties (i.e., businesses, research institutions, Government and private organizations, individuals, and other types of legal persons) on our Entity List and are therefore subject to restrictions on the items they can receive. Over 300 of those were added during the Biden-Harris administration, which has added more PRC parties to the Entity List than any prior Administration. They have been added for reasons including supporting the PRC's military modernization and WMD programs, supporting Iran's WMD and military programs, facilitating human rights abuses in Xinjiang, and providing restricted items to Russia. These parties include those involved in AI, surveillance, biotechnology, microelectronics, and quantum computing.

Engaging International Partners

The United States has relied on and acted in close cooperation with its allies and partners to bring together the international community to address military aggression, threats to sovereignty, and human rights abuses around the world. These last few years, we have doubled down on efforts to invigorate our international partnerships and taken broad efforts to liberalize controls for our allies and partners.

While we address the challenges posed by the PRC, Russia's brutal invasion of Ukraine has reinvigorated our close and continuing international partnerships. Technology supply chains span across borders, and technological expertise is dispersed throughout the world. The best way to truly keep potentially dangerous technologies and know-how out of the hands of bad actors is to work together. Coordinated controls reduce instances of evasion or backfill by other suppliers from other countries, ensuring that our controls remain effective over the long term.

Global Export Control Coalition

This is the approach we have adopted in building the Global Export Control Coalition, focused on using all aspects of export controls to degrade Russia's military capabilities, as well as those of enablers such as Belarus and Iran. This coalition—led by the European Commission, Japan, the United Kingdom and the United States—enabled us to drive new approaches to lower-level commodity controls on Russia and its partners, using Harmonized Systems codes to parse EAR99 items (i.e., low technology consumer goods). Further, through this partnership we have coordinated outreach to other countries in order to more forcefully combat illegal di-

version. We have worked together to track data, identify priorities, and provide a unified message against Russia’s unlawful war.

To date, the Biden-Harris administration has added 925 entities in Russia, Belarus, and numerous third countries for reasons related to Russia’s war on Ukraine.² Of those, over 200 parties have been added in the last year, including dozens of parties in China. BIS has virtually cut off these entities from U.S. trade, shutting down established Russian diversion routes and making it easier for law-abiding industry to avoid selling their commodities into high-risk diversion markets.

In addition, we have imposed Entity List restrictions on all Specially Designated Nationals (SDNs) that have been identified by the Department of the Treasury in certain Russia-related programs to ensure that U.S. items are not sent to SDNs by foreign parties acting outside the scope of Treasury controls. In addition, we have added new export controls to combat circumvention, such as by adding addresses used by the industry supporting offshore transshipment in Hong Kong to the Entity List, thereby incentivizing the corporate services industries to better scrutinize their offshore clients. We have expanded controls on previously uncontrolled business software for design and management. We have calibrated our controls to achieve our stated objectives—by narrowing a license exception used to facilitate civil telecommunication so that it is harder to abuse, or by adding a new License Exception for medical device exports serving humanitarian needs. We have simplified and harmonized our expanding Russia-related regulations so that they are easier to find and understand. We now require a license for most trade going to Russia, with export controls on thousands of classes of items, including all items described in 22 entire chapters of the harmonized tariff code. We have also reached out repeatedly to industry to better understand their supply chains and the challenges of export compliance.

Facilitating Exports and Reexports to Close Allies and Partners

In recognition of key allies’ and partners’ support of our efforts against Russia, along with their leadership in the areas of chemical and biological weapons non-proliferation and the promotion of human rights, EA removed license requirements for certain items going to close partners and allies, making it easier to facilitate exports and reexports involving these countries, and allowing BIS to apply its resources toward reviewing and monitoring more sensitive exports and higher-risk transactions. Related to that, we expect to publish a final rule streamlining license exception Strategic Trade Authorization (STA) in the coming months to realize the original goal of Export Control Reform in making STA a key facilitator of secure technology transfer and interoperability with allies and partners. This will build off the proposed rule published last year.³ These rules will also free up licensing resources to focus on higher-risk transactions.

To complement the State and Defense Department’s ongoing work to implement a broad defense trade exemption to advance the goals of the Australia-U.K.-U.S. Enhanced Trilateral Security Partnership, or “AUKUS”, we have already incorporated the premise of AUKUS into our export controls. We recognize the importance of the enhanced export control and technology protection measures enshrined in the United Kingdom’s National Security Act of 2023 and Australia’s Defence Trade Controls Amendment and Securing Australia’s Military Secrets Acts of 2024. Accordingly, effective April 19, 2024,⁴ we amended our export controls to remove nearly all remaining list-based license requirements for exports to Australia and the United Kingdom, expanded the availability of license exceptions, and eliminated certain end-use and end-user controls. These reforms will facilitate defense trade and technology cooperation with two of our closest allies and reduce burdens associated with licenses valued at up to \$7.5 billion per year.

Defense Priorities and Allocations System Title I of the Defense Production Act (DPA)

In addition to its export control functions, the Commerce Department has several responsibilities in implementing nonpermanent provisions of the Defense Production Act (DPA).

First, under Title I, the Commerce Department administers the Defense Priorities and Allocations System (DPAS). Second, under Title VII, the Commerce Department analyzes the health of U.S. industrial base sectors. Finally, also under Title VII, BIS

² <https://www.bis.gov/press-release/department-commerce-announces-additional-export-restrictions-counter-russian#:text=>

³ <https://www.federalregister.gov/documents/2023/12/08/2023-26681/proposed-enhancements-and-simplification-of-license-exception-strategic-trade-authorization-sta>

⁴ <https://www.bis.gov/press-release/commerce-significantly-streamlines-export-controls-australia-and-united-kingdom>

submits an annual report to Congress on offsets in defense trade. All three DPA authorities will expire if not reauthorized before September 30, 2025.

The DPAS establishes procedures for the placement, acceptance, and performance of priority rated contracts and orders for industrial resources, and for the allocation of materials, services, and facilities in support of approved national defense programs. The DPAS is regularly used to support the acquisition of industrial resources needed to support U.S. national defense requirements, especially by the Department of Defense.

The Commerce Department works closely with the Department of Defense to support the U.S. Armed Forces through the DPAS to ensure the timely delivery of industrial resources needed to support critical operational requirements and ensure our national security goals are met. We are very proud of the role we play to support our servicemembers through the DPAS. The Commerce Department may also authorize other Government agencies, foreign Governments, owners and operators of critical infrastructure, or U.S. or foreign companies to place priority ratings on contracts or orders on a case-by-case basis upon request. In response to these challenges, the Commerce Department, in coordination with the appropriate interagency partners, has responded to a significant increase in requests for assistance under the DPAS regulation.

For example, in 2023, the Commerce Department undertook 59 official actions in response to DPAS assistance requests, which is the highest number of official actions undertaken by the Department in the last 34 years. Fifteen of these rating authorizations were issued in support of U.S. Government Agencies, including three in support of Department of Defense programs and one in support of U.S. Government support to Ukraine. An additional 12 rating authorizations were issued in support of Commerce's memorandum of understanding with Canada to provide reciprocal military priorities support, eight of which were in support of Canadian defense procurements and four of which were in indirect support of Department of Defense programs. Within these 2023 activities, the Commerce Department, in coordination with the Department of Defense, also issued two rating authorizations in support of NATO and 26 rating authorizations in support of our foreign military partners, including 24 rating authorizations in support of Department of Defense's Security of Supply Arrangement partners, such as Israel, Italy, and the Republic of Korea. One of the rating authorizations issued to a Department of Defense Security of Supply Arrangement partner was ultimately in support of defense systems that would be transferred to the Ukrainian Ministry of Defense.

If the DPA's Title I authority were to lapse, the Commerce Department would no longer be able to support procurement on behalf of an entity other than the U.S. Armed Forces. Without DPA Title I, Commerce would rely only on the limited priority authority delegated to it under the Selective Service Act of 1948 to administer the DPAS.

The DPAS continues to facilitate the timely delivery of industrial resources to support U.S. national defense needs, including military and emergency preparedness programs, coalition partners, and increasingly, our Federal interagency partners. The Department of Commerce is eager to work with Congress to reauthorize the nonpermanent provisions of the Defense Production Act.

A Modern Export Administration

BIS is now at the center of strategic competition with the PRC over technologies that are critical to military advances. It plays a pivotal role in preventing foreign countries and entities of concern from leveraging American technology to develop items that can be used for strategic overmatch against the United States. There are more U.S. exports generally, more U.S. exports requiring a BIS license, and more export license applications submitted to BIS to be reviewed by the bureau and its interagency partners.

The emergence of adversaries with vastly more sophisticated tactics for evading or circumventing U.S. export controls has necessitated further calibration of export controls, which has further expanded the scope of BIS's work.

Accordingly, we have repositioned ourselves organizationally to match our substantially growing responsibilities. We implemented a new EA leadership framework to ensure we continue to effectively protect national security and appropriately manage policy engagement and implementation. Our internal review recognized two main channels of activity: strategic trade, which includes our licensing functions, as well as our outreach and training mission; and technology security, including our defense industrial base and Section 232 responsibilities, and all of the analytic work we do on licensing and trade data, industry research, and intelligence. Accordingly, we formally created a Principal Deputy Assistant Secretary (PDAS) to oversee all

of this work and two Deputy Assistant Secretaries (DAS)—one for Strategic Trade (ST) and one for Technology Security (TS).

In office organizational terms, the DAS/ST oversees the Offices of: Exporter Services, National Security Controls, and Non-proliferation and Foreign Policy Controls. The DAS/TS is responsible for EA's Offices of: Strategic Industries and Economic Security; and Technology Evaluation (OTE).

ECRA Section 1758 charges us with identifying and implementing appropriate controls on emerging and foundational technologies essential to national security. This critical part of our mission that demands dedicated resources and attention. This work, as well as foreign technology analysis and other research efforts designed to help assess the effectiveness of our export controls is being formalized under the DAS/TS. OTE leads EA's Section 1758 work, including through proactive research, analysis, collaboration and consultation with interagency partners and key industry and academic stakeholders, as well as supporting engagements with allies and partners at the regimes. Our nonproliferation experts, notably in the Chemical and Biological Controls Division have provided critical leadership in this space, through proposed rules on new technologies like peptide synthesizers. Formalizing a Technology Security branch of EA is essential for moving BIS from its historic focus on export control regulations towards a holistic approach of assessing the intersection of technology ecosystems, export control authorities, and national security and foreign policy goals.

Further enhancing this approach, under our new PDAS, we have formed an International Policy Office (IPO). Our vision for EA requires consistent and proactive engagement with our allies and partners to achieve mutual goals, as well as increased focus on the activities and plans of Nations that challenge global peace and security. IPO leads EA's increasing focus on engaging on a plurilateral and bilateral basis to address evolving threats. This Office is furthering and deepening BIS's many plurilateral and bilateral relationships, and enabling country-specific analysis not necessarily tied to a specific technology or multilateral regime.

BIS's national security mission is more important than ever in an era of dynamic strategic competition with the PRC and rapid technological advancement. However, funds appropriated by Congress for the bureau have remained flat—\$191 million—over fiscal years 2023 and 2024 despite the following challenges:

- From 2013 to 2023, total U.S. exports were up approximately 28 percent, and exports under BIS licenses are up approximately 222 percent.
- BIS license applications have also nearly doubled in the last decade; in recent years, BIS is processing more than 42,000 licenses per year, in contrast to just under 26,000 licenses annually in 2013.
- Our staff are relying on foundational systems for both license adjudication and enforcement work that were put in service in 2006 and 2008, respectively.
- License review timelines continue to increase, particularly to the PRC, as licenses become more complex, particularly for exports of electronic components.
- BIS's law enforcement arm, the Office of Export Enforcement, employs only 150 agents to counter the threat posed by Nation State actors, which means an increase in sworn law enforcement officers and analysts is overdue.

With the support of additional resources, BIS would be better able to meet the needs of the current geopolitical environment by enhancing these two channels of effort. Specifically, BIS has identified areas that would most benefit from additional resources, including:

- Information Technology (IT) systems and security modernization to secure and enhance BIS's infrastructure (including modernized digital management systems).
IT modernization would augment EA's ability to factor in all-source data during license application, including data generated by U.S. Government and the private sector. These updates would bolster the capabilities, capacity, and security of BIS data servers, facilitating comprehensive improvements to all aspects of BIS work that involve data intake and analysis—from evaluating the effectiveness of U.S. export controls to deploying supply chain analytic software to proactively identify and trace downstream supply chain diversion.
- Data and analytics, such as proprietary datasets and a modern data analytics system, to broaden BIS's understanding of how critical supply chains interact and the intricacies of entity-business relationships.
Access to more fulsome data would improve BIS's ability to analyze how trade flows, assess control efficacy and impact, and identify new technologies at their

inception. Improving EA's analytic capabilities in OTE and IPO, in particular, would strengthen and streamline impact across all bureau equities.

- Specialized, in-house expertise, including experts across critical fields and contracts with national labs and other relevant entities, to ensure that BIS stays up-to-date with cutting-edge technology and markets, as well as economics and supply chain management.
- Domestic and international policy engagement, including more cohesive inter-agency policy coordination and a new international engagement focus to continue building upon the multilateral partnerships that arose in the wake of Russia's full-scale invasion of Ukraine and that also support coordinated actions related to the PRC's semiconductor industry.

The need for new bilateral and multilateral partnerships will continue for the foreseeable future as the PLA aims to reinforce and consolidate its influence in critical global supply chains that span the Middle East, the African continent, Southeast Asia, and beyond. In order to sufficiently counter the threats posed by the PRC, BIS requires a significant and sustained increase in resources to further support accomplishing its critical national security mission. Such an investment by Congress in BIS is, fundamentally, an investment in U.S. national security. This investment will yield tangible results, and, in terms of importance, should be regarded in the same vein as the military and other traditional tools of power.

The status quo has shifted, as demonstrated by the unparalleled technological advances that have dramatically increased the need for national security and foreign policy controls and enforcement of violations. Agencies across the U.S. Government have ramped up capacity to tackle the concerns regarding China, and BIS needs additional resources and authorities to follow suit. With additional funding and authorities over the next 5 years, BIS could more effectively execute its mission and keep critical technologies out of the hands of foreign countries and entities of concern.

Conclusion

Dual-use export controls have never been more relevant or more effective at protecting our national security. We are focused on aggressively and appropriately contending with the strategic technology threat posed by the PRC and will continue to appropriately and aggressively use the tools at our disposal to counter PRC efforts to outpace the United States and our allies.

Thank you for inviting me to appear today. I look forward to continuing to work with you, and I am happy to answer your questions.

PREPARED STATEMENT OF PAUL ROSEN

ASSISTANT SECRETARY FOR INVESTMENT SECURITY, DEPARTMENT OF THE TREASURY

JULY 25, 2024

Good morning, Chairman Brown, Ranking Member Scott, and Members of the Committee. Thank you for the opportunity to provide an update on the work of the Treasury Department's Office of Investment Security (OIS) and the Committee on Foreign Investment in the United States, or CFIUS. I also want to thank Congress for the authorities and resources you have provided since the passage of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), as well as for the constructive and bipartisan support to our national security mission, which has helped make possible many of the enhancements that I will discuss.

CFIUS is a critical national security tool that enables thorough reviews of foreign investments in the United States for national security risks. The Committee—comprised of the heads of several Executive branch departments and offices and which I help lead as head of OIS in support of the Secretary of the Treasury's role as Chair—carefully reviews foreign investments in the United States for national security risks. When necessary, the Committee takes action to address any such risks while seeking to maintain an open investment environment and the status of the United States as the world's top destination for foreign direct investment.

Last year, I spoke to this Committee about our work. Among other things, I outlined how Treasury has implemented the FIRRMA reforms that overhauled CFIUS, and President Biden's September 2022 Executive order on Ensuring Robust Consideration of Evolving National Security by CFIUS. I spoke about how we have hired dedicated professionals to carry out this work, how we monitor compliance and enforce CFIUS requirements, and how we engage with our allies and partners. I also previewed our thinking in how we planned to address risks associated with certain

“outbound” investment from U.S. persons to countries of concern, such as the People’s Republic of China (PRC).

The progress and good work of Treasury and CFIUS continues, and this year, I want to further update the Committee on the status of this work as well as additional areas of progress. Let me start with an area that does not get as much public attention but is critical to our mission—our analytical and operational capabilities. Over the past 18 months, we have vastly improved our competencies in these areas. We have built and implemented sophisticated tools, platforms, and methodologies for assessing and addressing national security risks. We have employed cutting-edge information technology platforms to securely manage and facilitate novel aspects of CFIUS’s work. We have expanded and deepened our human capital, and today have a Treasury team with widely diverse backgrounds, from lawyers to science Ph.D.’s to intelligence professionals to bankers to compliance professionals and former prosecutors.

Many of the investments we are making benefit not just Treasury, but all of the Committee’s member agencies. For example, through our dedicated CFIUS funding established by Congress in FIRRMA, we are working with the interagency to enhance the Committee’s capabilities. This includes investments in modern information technology systems, data accesses, analytical tools, technical and industry studies, and staff training, to name just a few examples. These investments should pay national security dividends for many years to come.

Working to stay at the cutting edge in all of these areas has enabled us to be more efficient and effective even as we contend with two core challenges: transactions are becoming ever more complex in their structures and CFIUS is identifying and addressing more national security risks than in years past. Accordingly, CFIUS staff thoroughly scrutinize each notified transaction, peeling back the layers of the onion in pursuit of all the relevant facts regarding the foreign acquirers and U.S. targets all within statutory deadlines. We have paid particular attention to the role of limited partners in investment funds, as their access to, and influence and control over, sensitive businesses can vary considerably.

All while tackling these challenges, Treasury has successfully improved the efficiency of CFIUS’s operations. As noted in the latest CFIUS Annual Report, in 2023, CFIUS cleared 66 percent of filed declarations or notices within the first 30 or 45 days, respectively, compared to 58 percent in 2022. Another indicator of efficiency—the rate at which parties withdraw and refile their notices, also has fallen, declining from 23 percent of notices in 2022 to 18 percent in 2023, the first such decrease in 5 years. These changes are not incidental but instead reflect improved efficiencies, a cornerstone of our focus.

While efficiency is important, our core mission continues to be to identify national security risks arising from covered transactions and address them through enforceable orders, entering into mitigation agreements, or leveraging the President’s statutory authority to block or unwind a transaction. Our work does not stop after a mitigation agreement is signed—we work with the parties to ensure they comply with the agreement’s terms, and hold them accountable when they don’t.

Over the last 2 years, Treasury has transformed the way the Committee approaches compliance with mitigation agreements, and enforcement thereof. We have expanded and devoted significant resources to the monitoring and enforcement mission, including by nearly doubling the size of Treasury’s team over the last several years. Since 2022, Treasury and other CFIUS monitoring agencies have paid particular attention to compliance, including conducting in-person and virtual site visits here in the United States and abroad to probe and test compliance, and quickly refer matters for enforcement investigations where appropriate.

While our work to ensure compliance is critical, so too is making certain that companies know that CFIUS will enforce violations of mitigation agreements where appropriate. Treasury has led the Committee’s reinvigorated efforts to broaden, sharpen, and deploy CFIUS’s enforcement authority. In October 2022, Treasury issued CFIUS’s first ever enforcement and penalty guidelines. The guidelines are aimed at ensuring that transaction parties understand the Committee’s considerations and are held accountable for failing to comply with our laws and regulations, or for not upholding their obligations to address national security risk as part of mitigation agreements or orders, or other CFIUS regulatory requirements. In fact, in 2023, CFIUS assessed or imposed four civil monetary penalties for violations of material provisions of mitigation agreements, double the number of civil monetary penalties that CFIUS had previously issued across its nearly 50-year history. CFIUS has also, for the first time, issued subpoenas pursuant to its authorities to execute its national security mission.

While the Committee’s authorities are extensive, ultimately the power to prohibit or unwind a transaction lies with the President. Earlier this year, President Biden

ordered a Chinese cryptocurrency mining company, MineOne, to divest itself of a parcel of land in Wyoming that was in proximity to a military installation. This matter serves well to highlight the importance of CFIUS's efforts to identify transactions that were not notified to the Committee voluntarily and that may pose a risk to national security. The Committee leverages multiple tools to identify and analyze such non-notified transactions. Treasury's non-notified team screens thousands of potential covered transactions, ultimately putting forward to the Committee for consideration to request a filing those that may raise national security issues. The MineOne transaction came to the Committee's attention through our non-notified process in the form of a public tip.

Treasury also has led a number of regulatory enhancements to CFIUS's authorities. Over the last year, we have significantly bolstered CFIUS's jurisdiction over real estate transactions. As you know, CFIUS has the authority to review acquisitions of real estate in or around ports, or within a certain proximity to military installations and other sensitive Government facilities identified on a list maintained in the CFIUS regulations. Working with our Department of Defense counterparts, in July, OIS issued a proposed rule to amend the list to add 59 installations, building off the eight installations we added in August 2023. These additions are the first since the regulations implementing FIRRMA, and they represent a significant expansion of our jurisdiction.

In addition to these real estate enhancements, in April, to better effectuate many of the enhancements discussed above, we published a proposed rule to sharpen our investigation and enforcement tools. Among other things, the proposed rule substantially increases the maximum civil monetary penalty for certain violations and expands the types of information CFIUS can require parties to submit when engaging with them on non-notified transactions. Once finalized, the updated regulations will help us more effectively deter violations, promote compliance, and swiftly act to address risks to national security.

In many instances, our tools work best when we collaborate and act with allies and partners. For example, if CFIUS indicates that it will not approve an investment in a sensitive technology, the investor may try to "get around" CFIUS by making a similar investment in an allied country. In 2023 and 2024, CFIUS has had more than 300 engagements with allies and partners, and since 2019, approximately 30 countries have proposed, enacted, or significantly revised their foreign investment review regimes with our support. Last year, we worked with the Government of Mexico to sign a Memorandum of Intent to establish a bilateral working group on investment screening with Treasury.

Lastly, I want to turn from CFIUS to update you briefly on Treasury's efforts to address risks associated with certain outbound investments from the United States into other countries. Secretary Yellen tasked my office with implementing the President's new Outbound Investment Security Program pursuant to Executive Order (E.O.) 14105. The E.O. directed Treasury to issue regulations on outbound U.S. investment into certain sensitive technologies and products in identified sectors within countries of concern.

Treasury issued an Advance Notice of Proposed Rulemaking in August 2023 and received 60 public comments from a variety of stakeholders implicated by the E.O. We also have encouraged our partners and allies to consider taking similar action, as a multilateral effort will increase the effectiveness of stemming the flow of support to sensitive technology sectors in countries of concern.

Based on the feedback on the ANPRM, Treasury issued a proposed rule last month. My office will closely review the comments and prepare a final rule for publication. The program's success ultimately will depend on the resources we receive, and, to that end, I ask Congress to fully support Treasury's request for \$16.7 million in the President's FY25 budget for this program.

We are proud of Treasury and the Committee's efforts over the last 2 years, but our work remains unfinished. We remain focused on promoting and enforcing compliance with our regulations and agreements, improving our efficiency, and honing our authorities. I look forward to answering any questions you may have.

PREPARED STATEMENT OF GRANT HARRIS

ASSISTANT SECRETARY FOR INDUSTRY AND ANALYSIS, DEPARTMENT OF COMMERCE

JULY 25, 2024

Chairman Brown, Ranking Member Scott, distinguished Members of the Committee, thank you for inviting me to testify today. As stated by Secretary Raimondo, every day at the Commerce Department, we are tackling our Nation's most pressing

economic and national security priorities, and I welcome the opportunity to discuss how we are advancing this work.

As Assistant Secretary of Commerce for Industry and Analysis, I lead a team of more than 265 industry experts and economists. Our mission is to support the global competitiveness of U.S. industry. We provide critical sectoral expertise to proactively help U.S. industries compete abroad; strengthen supply chains vital to U.S. national security and economic competitiveness; advance U.S. exports and support job creation; and analyze investments to protect U.S. national security. The Industry and Analysis unit's work supports \$170 billion in U.S. exports and inward investment and over 595,000 American jobs (in FY23) and influences policy decisions affecting trillions of dollars of economic activity.

The Industry and Analysis business unit, which sits in the International Trade Administration, is the analytical engine of U.S. competitiveness policy because it has the broadest industry expertise and connectivity available in any one place in the U.S. Government, covering approximately 90 percent of the U.S. economy. We work on everything from raw materials like critical minerals, to vital components like semiconductors, to finished goods like autos and airplanes.

Understanding sectors and the ties between them is crucial to our Nation's economic competitiveness and national security priorities. This is why the Industry and Analysis unit's deep industry expertise, our unique commercial and national security perspective, and our advanced analytics capabilities are critical to advancing U.S. Government work on outbound investments, the Committee on Foreign Investment in the United States (CFIUS), and supply chain resilience.

Outbound Investment Security Program

The Outbound Investment Security Program addresses a crucial gap in existing national security authorities. Already, Commerce Department colleagues at the Bureau of Industry and Security (BIS) use export controls to regulate the transfer of commodities, software, and technology that threaten our national security. We also have sanctions programs administered by the Treasury Department that restrict the flow of U.S. capital, technology, and services to designated persons. Now, through the President's actions, we will soon have the Outbound Investment Security Program to prevent U.S. private capital from supporting advances in countries of concern in critical sectors that undermine U.S. national security.

The Commerce Department, and the Industry and Analysis unit in particular, plays a vital role in supporting the Outbound Investment Security Program called for by Executive Order 14105, "Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern", in August 2023. The Outbound Investment Security Program—like the CFIUS review process, which I will discuss subsequently—will be administered by the Treasury Department, but Commerce plays a significant role in each, leveraging our deep understanding of industries and supply chains.

In fact, from the start, the Administration's development of an Outbound Investment Security Program has relied on Commerce's core commercial and sector-specific technical expertise and, as recognized in the President's Executive order, Commerce plays a special role in supporting the program.

I would like to briefly describe three dimensions of our work on this program in more detail.

First, Commerce is key to identifying and understanding the relevant technologies that ought to be covered and how the requirements should be scoped. My team in Industry and Analysis has experts leading efforts to advance the global competitiveness of digital, information, communication, and other emerging technologies. We also have the technical fluency and industry relationships to help understand and anticipate national security risks associated with cutting-edge technologies—both those currently covered and those that may need to be recommended to the President for future inclusion. This includes, for instance, having the skillsets to understand the semiconductor and other critical supply chains to identify the full range of investments that could boost the military, intelligence, surveillance, or cyber-enabled capabilities of countries of concern while trying to prevent unnecessary economic disruptions.

Second, Commerce brings a unique commercial perspective and expansive industry connectivity. We have regular touchpoints with companies and business associations operating in sectors directly impacted by the regulations. In addition, my team spearheaded industry engagement on the Outbound Investment Security Program and, in coordination with Treasury, consulted over 450 stakeholders in multiple rounds of outreach designed to solicit feedback as the development of the program progressed. We sought out perspectives from companies and investors on how they

anticipate the program will impact their work, which is key as we seek to craft an effective program while reducing the risks of unintended market effects.

Third, Commerce will be key to successful implementation of the program. Our sector-specific experts will be indispensable to interpreting and recommending actions based on analysis of the influx of data that the private sector will be providing to the U.S. Government regarding outbound investments and associated supply chains. Going forward, we will play an important role in assessing whether to add or remove technologies and products covered by the program. In addition, we will help anticipate and propose policy adaptations if countries of concern seek to develop new mechanisms to evade scrutiny and access U.S. investment to advance technologies in a way that threatens our national security.

At Commerce, we understand that there is significant work ahead in the implementation of this program. We are focused on narrowly scoping the program to avoid unintended consequences and minimize negative impacts to the broader economy. We will continue to support the program to address national security concerns in a targeted and proactive way.

CFIUS

Industry and Analysis is the policy lead for the Department of Commerce's participation in CFIUS national security reviews. We provide indispensable sectoral and supply chain expertise that guide U.S. Government decisions in reviewing hundreds of billions of dollars of foreign investment, all while enhancing investor confidence in our Nation's longstanding open investment policy.

Since Congress enacted the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), the Industry and Analysis unit expanded its CFIUS team and established an Office of Investment Security. Our team has a wide range of experience in the public and private sectors, and we especially value these diverse backgrounds and skillsets as we work on increasingly complex CFIUS national security reviews. At the same time, we have taken on a greater leadership role on the Committee. As one example, since FIRRMA, Commerce has acted as a CFIUS lead agency on a significant number of CFIUS filings.

Overall, Commerce takes a broad approach to reviewing CFIUS cases. The Industry and Analysis unit provides analysis of issues related to the U.S. business and the market in which it operates, market trends, supply chain impacts, and the business rationales for transactions, among other issues. We also draw on inputs from across all of Commerce's bureaus and offices. In particular, my team works very closely with our colleagues in BIS, which reviews transactions with a focus on export control, technology transfer, and defense industrial base issues.

In Executive Order 14083, "Ensuring Robust Consideration of Evolving National Security Risks by CFIUS", issued in September 2022, President Biden directed CFIUS to consider supply chain resiliency in our national security analysis. Consistent with this direction, the Industry and Analysis unit examines a range of factors when considering whether a transaction may impact the resilience of certain critical U.S. supply chains, which may have national security implications. We consider issues such as the scale and types of supply relationships pertaining to a given U.S. company and the potential for supply chain disruption or undue foreign influence over specific supply chains. Analysis of supply chain risk in the context of investment reviews is part of a broader initiative by Industry and Analysis to advance the resiliency of U.S. supply chains, which I would like to briefly turn to next.

Supply Chains

The Industry and Analysis unit has long been central to U.S. supply chain work because of its breadth of sectoral expertise; its unique understanding of the opportunities and challenges facing U.S. companies; its daily connectivity to U.S. industry; and its economic analysis and modeling capabilities. In fact, we have had a supply chain services-focused office for over a decade and, for years before that, a dedicated team. We also have had an Advisory Committee on Supply Chain Competitiveness since 2011. Yet the criticality of this work has increased further still in recent years.

At its core, the Industry and Analysis unit focuses on applied analysis and action. For instance, the Industry and Analysis unit was the first team in the U.S. Government to sound the alarm on competitiveness in the semiconductor supply chain and spring into action. The team subsequently mapped out chokepoints, created an early warning system for industry to provide alerts of potential disruptions, and, in the face of severe shortages, connected industry leaders with semiconductor suppliers to encourage solutions. The team also set to work supporting investment to strengthen the supply chain and helped secure critical U.S. investments, such as those by Taiwan semiconductor companies totaling \$34 billion and supporting more than 20,000

U.S. jobs. And those investments in semiconductors have only grown, thanks to the CHIPS and Science Act.

Last year, we established what the White House called a “first-of-its-kind” Supply Chain Center to integrate industry expertise and data analytics to develop innovative supply chain risk assessment tools, coordinate deep-dive analyses on select critical supply chains, and drive targeted actions to increase resilience and address foreign dependency vulnerabilities. We aim to be the analytic engine for supply chain resilience policy by helping the U.S. Government be more proactive in getting ahead of supply chain challenges and strategic in setting priorities for action based on data-driven risk analysis. We also provide strategic and technical advice to other departments and agencies related to industry- and sector-specific competitiveness issues as they disburse billions of dollars in U.S. Government investments related to supply chains.

As part of this work, we are pioneering new data-driven tools and creating playbooks to assess supply chain vulnerabilities in specific sectors, including for emerging technologies. Our Supply Chain Exposure Tool provides a common operating picture of risks that enables focused, evidence-based conversations and actions with international partners. We are also building a tool that utilizes a comprehensive set of indicators to assess current or prospective supply chain risk across the U.S. economy, with an emphasis on risks to national security and economic security most relevant to the U.S. Government.

Additionally, we are providing action-oriented analyses on a wide variety of trade and supply chain related issues, including the impact of global supply chain disruptions, tariff actions, and unfair trade practices by the People’s Republic of China. We are supporting industry resilience to supply chain or geopolitical shocks and working with foreign Governments to mitigate international supply chain challenges. We are also supporting work targeting tens of billions of dollars of export opportunities for U.S. industry and inward investment to the United States as part of strengthening high-priority supply chains.

These efforts, which leverage the critical FY23 funding provided by Congress, are central to U.S. Government efforts to be more strategic and proactive in strengthening supply chains and securing our national interests. This work supports U.S. economic competitiveness and domestic job growth while supporting U.S. businesses in leading the industries of the future. At the same time, it is vital to improve our ability to counter efforts by adversaries to gain or exercise strategic leverage over key supply chains.

Conclusion

I appreciate the opportunity to update the Committee on Commerce’s efforts to safeguard U.S. national security and economic competitiveness through our work on outbound investment, CFIUS, and advancing supply chain resilience.

If I have sought to convey one thing, it is this: I believe that industry expertise, and the ability to look across sectors, is vital to investment security, protecting and promoting U.S. technological advantages, supporting domestic manufacturing and job growth, and addressing attempts by adversaries to weaponize supply chains. For these reasons, the singular industry depth and connectivity of the Industry and Analysis business unit at Commerce has never been more central—or more needed—to protecting and advancing U.S. economic competitiveness and national security.

To meet these growing demands and, more frankly, to meet U.S. economic and national security needs, these efforts require resources. The President’s FY25 Budget Request for the International Trade Administration is \$645.5 million. This includes \$5 million in new funding to support the Outbound Investment Security Program so that we can provide the sectoral and commercial expertise, industry connectivity, and actionable recommendations to ensure that the U.S. Government can understand and act on information received from covered transactions while also minimizing the risk of unintended disruptions to U.S. business. The President’s Budget Request also includes \$12 million to sustain and support our supply chain resiliency efforts. This support is needed to improve crisis response and anticipate future constraints in key sectors so that the U.S. Government can proactively strengthen critical supply chains. Unfortunately, the House FY25 mark only provides the International Trade Administration \$558 million, which is \$53 million (9 Percent) below the FY24 enacted level and \$87.5 million below the President’s Budget Request.

As Congress works to finalize the FY25 appropriation bills in the coming months, we ask that you please consider how important it is for U.S. national security to support and fully fund these functions. Thank you for having me here today. I look forward to answering your questions.

PREPARED STATEMENT OF LAURA TAYLOR-KALE
ASSISTANT SECRETARY FOR INDUSTRIAL BASE POLICY, DEPARTMENT OF DEFENSE

JULY 25, 2024

Good morning, Chairman Brown, Ranking Member Scott, and Members of the Committee. Thank you for the opportunity to testify today on the state of the defense industrial base, and the ways in which the Defense Production Act (DPA) can be used to address shortfalls and adversarial capital investments in the defense industrial base. I look forward to highlighting today how DoD links systemic and emerging economic threats to the defense industrial base with DPA investments in capacity-building and defense supply chain resilience. To ensure that we are protecting and expanding our defense industrial base, the DoD strongly supports the reauthorization of the Defense Production Act. Supporting the Defense Production Act is one of the most important actions that the Congress can do to ensure that the U.S. industrial base is ready to support defense needs and the Warfighter in addition to timely, consistent appropriations and multiyear procurement authority.

State of the Defense Industrial Base

Today we face geoeconomic and technological competition with peer and near peer adversaries that impact our economy and military posture. Defense production—undergirded by a strong industrial and innovation ecosystem—deters our adversaries. Since Congress enacted the DPA in 1950, the Executive branch has invoked DPA authorities to manage the Nation’s defense-related production capacity, defense critical supply chains, and to protect and strengthen the U.S. industrial base in war, peace, and during national emergencies. The DoD uses the DPA every day in its mission to safeguard vital U.S. national interests. Fully executing DPA authorities is a priority for defense industrial policy. In January of this year, the DoD published the first ever National Defense Industrial Strategy, which highlights four strategic priorities for building a modernized, resilient industrial ecosystem that can support national defense: (1) resilient supply chains, (2) workforce readiness, (3) flexible acquisition strategies, and (4) economic deterrence. The DPA is a critical tool for national defense and the successful implementation of the National Security Strategy, the National Defense Strategy, and the National Defense Industrial Strategy.

As the first Senate-Confirmed Assistant Secretary of Defense for Industrial Base Policy, some of my top priorities includes overseeing DoD’s participation in the Committee on Foreign Investment in the United States (CFIUS), addressing the impacts of malign economic activity on the defense industrial base, and the effective management and execution of DPA authorities and appropriations. I would like to thank the Congress for adding the United Kingdom and Australia to the definition of domestic sources for Title III awards in the FY 2024 National Defense Authorization Act. Allowing the DoD to enter agreements with companies the U.S., Canada, U.K., and Australia reinforce important alliances and the short- and long-term development of secure defense critical supply chains. Going forward, the DPA will remain a critical national defense tool to mitigate supply chain risk vulnerabilities in our key weapons and defense systems, and for building capabilities with close global allies and partners.

Addressing Supply Chain Shortfalls and Adversarial Capital Investments in the Defense Industrial Base

Our adversaries attempt to exploit supply chain vulnerabilities to weaken the U.S. economy and military. These systemic, ongoing threats take many forms, including economic statecraft, coercion and predatory investments and acquisitions by malign actors who seek to undermine our national security and defense, weaken the defense industrial base, and erode our military advantage. My office often identifies these risks through our review of CFIUS transactions, Hart-Scott-Rodino mergers, and other economic-focused matters. Through these authorities, we catalogue actions that must be taken to ensure that adversarial capital investments do not rob the U.S. industrial base of technology and capability leadership.

As a key pillar of the National Defense Industrial Strategy, economic deterrence is the DoD’s strategic focus approach to economic security that promotes defense industrial resiliency and capacity. Economic deterrence efficiently integrates policies, investments, countermeasures, and other risk mitigation activities inside and outside the DoD to prevent adversaries from weakening the defense industrial base by exploiting vulnerabilities and our open market economy. Our objective is to quickly identify and counter malign economic activities that threaten U.S. national security.

The DoD frequently uses DPA VII authorities to combat adversarial investments and predatory acquisitions in the U.S. industrial base. DoD is one of the most active members of CFIUS. While reviewing investment transactions, DoD is particularly

concerned with protecting military installations, supply chains, and technology from foreign ownership and influence. CFIUS caseloads have reached all-time highs in recent years. The DoD has dedicated significant time and resources to the successful execution of CFIUS authorities, and DoD is co-lead agency on a large proportion of all CFIUS cases. Additionally, DoD actively evaluates “non-notified cases”—transactions that were not submitted to CFIUS for a review or assessment. My team evaluates many such transactions and refers non-notified transactions to Treasury every year.

My team’s due diligence in investment and acquisition reviews includes intelligence, open-source information, cyber security analysis, counterintelligence, and business analytics to gather information on systematic vulnerabilities in defense-critical supply chains. By layering multiple sources of information, the DoD builds a holistic understanding of targets for adversarial investments, identifies defense sectors and technology capabilities that are most at-risk, develops mitigation strategies, and seeks to identify investment opportunities for DPA investments.

Leveraging analytics and intelligence from economic security reviews enables our decision-making for investments in industrial capacity-building. This integrated approach to assessment, analysis, strategy, and mitigation informs DoD’s primary use of the DPA—to increase the readiness and resilience of defense industrial base in support of defense critical needs and the Warfighter. Through informed investments and mitigation activities, DoD continues to ensure our Nation’s industrial base is dynamic, state of the art, resilient, and able to provide our Warfighters the capabilities needed to counter new and emerging threats and to prevail in conflicts.

Prioritizing Industrial Resources for National Defense: DOD Use of DPA Title I Authorities

The DoD utilizes DPA Title I authority through the Commerce-administered Defense Priorities & Allocations System (DPAS) to prioritize contracts and orders in support of DoD’s needs within industrial supply chains and to allocate scarce components to spur production and support allies and partners. This prioritization ensures that defense programs do not experience supply chain disruptions that inhibit meeting their program objectives in day-to-day operations and national emergencies. The DoD places DPAS priority rated contracts and orders for industrial resources over 300,000 times a year at no cost to the taxpayer to help ensure DoD procurements meet cost, schedule, and performance parameters by proactively mitigating supply chain risks.

Since the last DPA reauthorization in 2018, the DoD has leveraged Title I authority to directly contribute to national defense and prioritize the delivery of weapons and materiel to allies and partners. The DoD has signed 17 Security of Supply Arrangements (SOSAs)—nonbinding, reciprocal agreements to provide mutual support for industrial resources, including seven new SOSAs in 2023 with Japan, Israel, Latvia, Denmark, Lithuania, Estonia, and Singapore. The DoD has also endorsed Special Priorities Assistance requests for DPAS rating authority to Commerce to expedite delivery of military supplies at any level of the supply chain to allies. For example, in 2023, DoD endorsed the use of DPAS priority rating Title I authority to formally resolve 37 requests for Special Priorities Assistance. Two of these requests were in support of Ukraine-related efforts, including cases which supported the National Security and Defense Council of Ukraine’s cybersecurity infrastructure, prioritized the delivery of tanks, and expedited the manufacturing and transfer of more than 20,000 radios and other communications capabilities.

Expanding Production and Enabling Resilient Supply Chains: DOD Use of DPA Title III Authorities

Sufficient investment in the defense industrial base is critical to ensuring that the defense industrial ecosystem can produce at speed and scale. The DoD’s DPA Title III program is a key investment tool to build capacity and strengthen the defense industrial base. Single source and no source risk exists in nearly every supply chain and at all levels of the defense industrial base. It is a national security priority to sustain essential single source defense component manufacturers as well as mitigate sourcing risk upstream in supply chains. Through the use of Title III, DoD alleviates pain points in supply chains and expand domestic capacity in manufacturing, critical technologies, critical minerals and strategic materials, and vital defense capabilities. Industry demand is high for Title III support. Since the start of 2021, my office has received hundreds of proposals and favorably evaluated more than 50 projects (valued at \$5.74 billion). This fiscal year alone, DPA Title III has received over 140 industry white papers requesting a total of \$1.26 billion in Government funding, an increase from 15 white papers in FY21. Continued support of the U.S. industrial and technological base ensures that the United States has a resilient in-

dustrial ecosystem that serves as a deterrent to our adversaries. We will continue to work to ensure that taxpayer resources fund the best value for defense needs.

Title III Execution Since 2018

Congress has markedly increased DPA Title III appropriations in recent years. In FY 2018 and FY 2019, the DoD's DPA Title III appropriations, including Congressional adds, totaled \$67.4 and \$53.6 million respectively. Since FY 2020, DoD Title III appropriations have averaged over \$783 million which includes supplemental funding. The key factors driving increased DoD Title III budget has been the Government's response to COVID and DoD's urgent focus on shoring defense critical supply chains and expansion of domestic manufacturing capacity.

COVID Response

In March 2020, the Coronavirus Aid, Relief, and Economic Security (CARES) Act appropriated \$1 billion to the DoD DPA program to prepare for, prevent, and respond to coronavirus. In coordination with Health and Human Services (HHS), \$900 million of the \$1 billion in CARES Act funding was used to expand or maintain capacity in medical resources and the defense industrial base. DoD obligated a total of \$740.6 million (or 82 percent of the \$900 million) within the first 6 months and obligated much of the remaining funding over the next fiscal year. By FY 2022, appropriations totaled nearly \$1.4 billion as Congress and the Biden administration increased DPA appropriations to expand domestic manufacturing capacity, protect defense-critical supply chains from adversaries, and counter predatory investment and acquisition strategies.

Focus on Defense Supply Chain Resiliency in FY 2023 and FY 2024

Improving prioritization and execution of Title III programs has been an Administration priority and DoD has aligned Title III execution to Executive Order 13806 (Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States), Executive Order 14017 (America's Supply Chains), and the National Defense Industrial Strategy. The DoD has prioritized using Title III to expand domestic capacity in the most sensitive materials and critical minerals vital to national security, thereby reducing reliance on adversarial foreign sources, and tackling the long lead times of critical materials that inhibit industry's rapid production of key weapons systems. For example, DoD has obligated approximately \$20 billion to replace U.S. stocks and services drawn down for Ukraine, including Guided Multiple Launch Rocket Systems (GMLRS), Stinger, Javelin, and 155mm ammunition.

It is important to underscore that the DoD cannot exercise Title III authorities unless the President has issued a formal determination or waiver that an industrial resource, material, or critical technology item is essential to the national defense. Since the 2018 DPA reauthorization, the President has issued 22 determinations and three waivers. President Biden's February 2023 Supply Chain Waiver has been the most far-reaching in allowing DoD to swiftly act to avert shortfalls in defense-critical supply chains and quickly execute Title III awards.

As a result of the 2023 Presidential Supply Chain waiver, in FY23 the DoD executed \$733 million in DPA Title III awards that helped to strengthen supply chain resilience across sectors, including:

- *Microelectronics (\$22 million)*: Investments were made to sustain and/or expand manufacturing capabilities and establish a robust domestic microelectronics ecosystem in support of radiation-hardened microelectronics, printed circuit boards, advanced packaging, discrete components, and other electronics.
- *Strategic and Critical Minerals and Materials (\$329 million)*: Established and expanded domestic industrial mining, refining, processing, and manufacturing capabilities required to field weapon systems, including rare earth elements required for magnets, energetic materials required for munitions, structural materials for aircrafts, and upstream battery materials.
- *Kinetic Capabilities (\$351 million)*: Expanded existing production and onshore capabilities for critical chemicals required for DoD missiles and munitions; increase capacity for ball bearings and solid rocket motors for missiles and munitions.
- *Energy Storage and Batteries (\$31 million)*: Invested in domestic battery cell manufacturing capabilities to enable the Department to have a stable, qualified, and secure supply.

In FY 2024, the DoD is on-track to execute over \$1 billion in DPA Title III awards and continues to remain postured to execute the authorities provided under the DPA to support the Warfighter. DoD announced \$192.5 million in DPA Title III

awards in February 2024 to establish, expand, and modernize capability to manufacture 22 defense-critical chemicals and reduce reliance on foreign sources, particularly the PRC. These awards will result in production of several chemicals deemed critical for the proper functioning of defense and weapon systems. Many of these chemicals are also used in numerous commercial applications (including but not limited to pharmaceuticals, consumer products, agriculture, automotive, and energy), resulting in products that will be competitive in the marketplace and increase resiliency of domestic critical chemical supply chains.

Improving Title III Execution by Launching Defense Industrial Base Consortium Other Transaction Authority

The rapid scaling of DPA appropriations following the COVID supply chain crisis and Russia's invasion of Ukraine strained DoD's internal capacity to swiftly execute Title III awards. It has been my priority to quickly improve execution and align the Department's use of the authorities to the implementation of the National Defense Industrial Strategy. To that end, in January 2024, the DoD announced the establishment of the Defense Industrial Base Consortium (DIBC) Other Transaction Authority (OTA).

Along with the Air Force Executive Agent, DoD's launch of the DIBC OTA positions the DoD to shorten the time of execution of DPA awards and lessen bureaucratic hurdles. The OTA directly aligns with the NDIS four strategic priorities by providing a vehicle to rapidly research, prototype, and manufacture commercial solutions for defense requirements and innovations from private industry, academia, and firms not traditionally part of defense contracting systems. The OTA will spur competition and attract nontraditional defense contractors, nonprofit research institutes, and small businesses that will in turn lead to an expansion of the defense industrial ecosystem, increase innovation, and improve the transition of new technologies into production. Additionally, the OTA can execute interagency requirements aimed at enhancing critical domestic supply chains.

Fully Executing DPA Title III Authorities: Reauthorization Priorities for DOD

DPA strongly supports the reauthorization of the DPA as the Department continues to use DPA authorities to advance national security and mitigate to the defense industrial base and the U.S. technological innovation ecosystem. DPA Title III authorizes the use of direct purchases (grants), purchase commitments, guarantees of purchases or leases of advanced manufacturing equipment, and loans or loan guarantees. Currently DoD only has the capacity to issue Title III grants for direct purchases. Essentially DoD only uses one of the four Title III authorities. However, we need to fully use DPA Title III to mitigate systemic and emerging threats to national defense. To support fully executing the potential of DPA authorities, the DoD requests two key changes to the existing DPA law to respond to increasing requirements. We submitted these legislative proposals to Congress. Specifically, the DoD supports legislative amendments that would raise the DPA annual fund balance and remove designation of the Secretary of the Air Force as the sole and exclusive executive agent.

First, raising the DPA Fund annual fund balance ensures that the DPA Title III Program will not be penalized for increased and supplemental appropriations. DoD increasingly leverages DPA authorities to respond to critical national defense requirements, the balance of the DPA Fund is anticipated to rise accordingly. While the DPA Title III Program always pursues the most expedient path to execution, some acquisition or mitigation strategies cannot be completed in the span of a year. As such, DoD requests amending the law to allow for a higher DPA Fund balance so that monies that are appropriated or transferred into the DPA Fund are not returned to the Treasury.

The second change that the DoD supports is the elimination of the sole and exclusive Executive Agent in favor of access to multiple execution offices. The designation of the Secretary of the Air Force as the sole and exclusive DoD executive agent for the DPA Title III program unnecessarily constrains the ability of the program to execute efforts in support of national security requirements. While we will continue fully utilizing the Air Force resources devoted to DPA execution, the increased appropriations to the program require DoD to use all available contracting mechanisms to expediently obligate funds. Amending the designation of the Secretary of the Air Force as "the sole and exclusive Department of Defense Executive Agent" to "an execution office for the Department of Defense" would allow seamless access to additional execution offices for the DPA Title III program, enabling the Department to leverage additional contracting resources when necessary.

Finally, DoD supports increasing the period of availability of Title III funds. Currently, DoD only issues direct purchase grants due to the recent change in period of availability for appropriations from non-expiring to 5 years in the last Appropriations Acts. If Congress appropriates non-expiring funds in the future, DoD can issue purchase commitments, loans, and loan guarantees through DPA authorities. Purchase commitments would particularly improve defense supply chains by helping to spur advanced procurement of critical materials and make DOD demand more predictable.

Closing

In closing, DPA is critical to ensuring that America is ready to address shortfalls and counter adversarial capital investments in the defense industrial base. The DoD will continue to focus on increasing execution of DPA Title III funding and look for opportunities to utilize more of the authorities to include purchase commitments, loans, and loan guarantees. I cannot over-emphasize how important the DPA is to ensure that the DoD can protect and strengthen the U.S. industrial base, and work with our closest allies and partners to secure defense-critical supply chains. We look forward to working with Congress and the interagency on the successful reauthorization of the DPA and support for DoD legislative proposals to fully align DPA execution with the defense critical needs.

**RESPONSES TO WRITTEN QUESTIONS OF CHAIR BROWN
FROM THEA KENDLER**

**Questions for the Record from Chair Sherrod Brown
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
Committee on Banking, Housing, and Urban Affairs
Thursday, July 25, 2024**

1. The National Security Commission on Artificial Intelligence called artificial intelligence the quintessential dual-use technology. AI continues to advance rapidly, and preventing China’s military and intelligence services from accessing advanced artificial intelligence technology is a national security imperative. Are there any additional authorities or resources BIS needs to ensure that our export controls keep advanced AI technology from getting into the wrong hands?

Response:

The Bureau of Industry and Security (BIS) has imposed unprecedented restrictions on the People’s Republic of China’s (PRC’s) access to advanced semiconductor manufacturing equipment, chips and other items needed to develop advanced AI capabilities that present U.S. national security concerns. Furthermore, BIS has prohibited U.S. persons from supporting chip development and production that power AI systems at certain semiconductor fabrication facilities located in Macau or Country Group D-5 (U.S. Arms Embargoed Countries) without a license. However, we know that the PRC is looking for ways to continue accessing these high-end chips.

The Department of Commerce welcomes the opportunity to continue working with Congress to ensure BIS has sufficient tools to protect our national security and prevent the PRC from acquiring sensitive technologies, such as AI, that could advance its military, intelligence, surveillance or cyber-enabled capabilities, as well as impair Russia’s and Iran’s ability to acquire foreign produced chips.

Additionally, BIS strongly urges Congress to take the crucial step of enacting the 2025 President’s Budget request for \$223.392 million at the agency, including an \$8 million program increase for export control policy analysis and engagement, an \$8 million program increase for export enforcement, an \$8.892 million program increase to properly implement E.O. 14110 on artificial intelligence, a \$4 million program increase to enhance critical data fusion, analytic, and decision-making capabilities, and \$3.5 million to start modernizing BIS’s IT systems.

2. As part of the FEND Off Fentanyl Act, Congress amended the International Emergency Economic Powers Act to extend the statute of limitations for sanctions enforcement investigations from five years to ten years. Would extending the statute of limitations for export control enforcement from five years to ten years strengthen our export control system? If so, how?

Response:

Export enforcement and sanctions enforcement work in concert with one another. In fact, ECRA includes language directing the coordination of sanctions and export control authorities. An extended statute of limitations for ECRA would likely result in more robust export enforcement.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR SCOTT
FROM THEA KENDLER**

**Questions for the Record from Ranking Member Tim Scott
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
Committee on Banking, Housing, and Urban Affairs
Thursday, July 25, 2024**

1. Ms. Kendler, Hamas’ savage terrorist attack on Israel and Israel’s defensive response has led some nations, such as Turkey, to place boycotts on Israel and have fueled antisemitic rhetoric across the globe. We are now seeing foreign nations asking U.S. firms in areas such as shipping and logistics to participate in the boycott of Israel to fulfill contracts. As Americans, we must strongly stand by our ally Israel, and we must do all that we can to fight antisemitism as it pops up around the globe.
 - a. Please provide an overview of the steps that you are taking to exercise BIS’ antiboycott authorities.
 - b. Additionally, please explain what you are doing to alert U.S. businesses to their antiboycott compliance obligations?

Response:

BIS’s Export Enforcement, led by my colleague Assistant Secretary Matthew Axelrod, administers and enforces the Anti-Boycott Act of 2018, Part II of the Export Control Reform Act of 2018 (ECRA), and the antiboycott provisions set forth in part 760 of the Export Administration Regulations, 15 CFR parts 730-774 (EAR).

In March 2024, BIS published a new resource, a list of entities who have been identified as having made a boycott-related request in reports received by BIS. This list is posted on BIS’s Office of Antiboycott Compliance webpage and notifies companies, financial institutions, freight forwarders, individuals, and other U.S. persons of potential sources of certain boycott-related requests they may receive during the regular course of business. The requester list is updated quarterly.

By publishing this list, BIS aims to raise awareness of the sources of past boycott requests, facilitate fulfillment of the antiboycott reporting requirements, and deter foreign parties from imposing – and U.S. parties from acquiescing to – boycott-related requests and conditions. In May 2024, in response to Turkey’s announcement that it would suspend all trade with Israel pending the resumption of humanitarian aid into Gaza and a ceasefire, BIS issued an Antiboycott Advisory reminding U.S. companies, wherever situated, of their responsibilities under the antiboycott regulations. The regulations prohibit taking certain actions in furtherance or support of an unsanctioned foreign boycott maintained by a country against a country friendly to the United States. Additionally, the regulations require reporting of receipt of a boycott-related request to BIS.

2. I am interested in better understanding the role your Department and your office played in implementing President Biden's Executive Order on Artificial Intelligence.
 - a. What is your overall takeaway from your Defense Production Act survey of the artificial intelligence industry?
 - b. How many private sector companies did the Commerce Department contact to implement the Defense Production Act provisions for the President's Artificial Intelligence Executive Order?
 - c. What data or information did the Commerce Department request from private companies through the Defense Production Act?
 - d. Could you please explain how business confidentiality in the Defense Production Act limits your ability to share collected Defense Production Act survey information with Congress? Please be specific.
 - e. Do you plan to ask to use any authorities under the Defense Production Act or International Emergency Economic Powers Act in relation to artificial intelligence?

Response:

BIS contributes to the implementation of the President's Executive Order (EO) on "Safe, Secure, and Trustworthy Use and Development of Artificial Intelligence" (EO 14110) through our activities under the Defense Production Act (DPA). We are instituting measures to enhance the national defense and national security as next-generation frontier Artificial Intelligence (AI) models are developed, including measures requiring developers to report the steps they are taking to test their models and protect them from theft. These measures build on the voluntary commitments that companies are making on safety, security, and trust – and will promote the safe development and use of AI. In accordance with EO 14110, BIS published a proposed rule on AI reporting requirements in September 2024.¹ The comment period closes October 11, 2024.

Under EO 14110, BIS conducted a survey of frontier AI developers and computer cluster providers. Information from this survey provides the Department and the U.S. Government with insights needed to understand the health and viability of the assessed industry sectors to support national defense. The assessment will provide findings and recommendations for government policymakers and industry leaders to support our national defense, by understanding and supporting a healthy and economically competitive U.S. industrial base.

¹ Establishment of Reporting Requirements for the Development of Advanced Artificial Intelligence Models and Computing Clusters, 89 Fed. Reg. 73612 (Sept. 11, 2024), <https://www.federalregister.gov/documents/2024/09/11/2024-20529/establishment-of-reporting-requirements-for-the-development-of-advanced-artificial-intelligence>.

EO 14110 set very high technical thresholds for participation in this collection. In order to be a part of this collection, a company must either have, be developing, or have short-term plans to develop a model trained with a massive amount of computing power or possess a highly advanced supercomputer. Only a small handful of computers and models meet these thresholds, which were set deliberately so that BIS would only be surveying those in possession of AI technology that could either provide important tools to bolster U.S. national defense and security, or potentially jeopardize it if they fell into the wrong hands.

BIS deployed this survey in January 2024 to fewer than 50 AI developers and computing cluster providers that we deemed likely to have crossed the technical thresholds for inclusion in this assessment laid out in the EO.

The survey collected information required under Section 4.2(a) of EO 14110. BIS asked a targeted series of questions to gather information about companies' plans to develop dual-use foundation models and the cyber and physical security activities companies were taking to protect the training process for these models; the ownership and possession of the weights for any dual-use foundation models, as well as the physical and cyber security measures taken to protect these weights; and red team test results evaluating a dual-use foundation model's potential to lower the barriers for the development of chemical, biological, radiological, and nuclear weapons, conduct an offensive cyber attack, use software or tools to influence real or virtual events, or self-replicate. The survey also asked computing cluster providers to disclose the existence of any large-scale computing clusters.

Pursuant to 15 CFR § 702.3, all information submitted in response to a Defense Production Act industrial base survey may not be released without a determination made by the Undersecretary for Industry and Security, the Secretary of Commerce, or the President that withholding this information would be contrary to the national defense. The survey document itself is treated as confidential due to national security concerns about the sensitivity of the assessment questions as well as the information being requested. This confidentiality helps ensure that BIS is providing our industry partners with the maximum amount of security.

Certain provisions of the Defense Production Act are scheduled to expire on September 30, 2025. The Department of Commerce is eager to work with Congress to reauthorize the non-permanent provisions of the Defense Production Act.

3. You oversee Defense Production Act surveys at the Commerce Department. Could you provide me with a list of non-defense industrial base areas where you see our industrial base falling short? Please be specific.

Response:

In recent years, Commerce has determined that it is necessary to conduct surveys and assessments on areas that do not fall under the traditional defense industrial base areas including on U.S. healthcare and public health preparedness and response capabilities – specifically related to influenza vaccine, U.S. civil space supply chain network, U.S. microelectronics, legacy semiconductors and chips, and AI developers and computer clusters.

Data collected by past Commerce surveys demonstrate that rare earth elements are a significant vulnerability. Rare earth elements are used in metallurgy, polishing, and the creation of catalysts and magnets, with a range of applications including automobile and petroleum refining, phosphors for flat panel displays in mobile phones and laptops, permanent magnetics, and rechargeable batteries, as well as fighter jet engines, missile guidance systems, lasers, and satellite communications systems. The U.S. share of rare earth element mining has declined precipitously, and today we are heavily dependent on the PRC.

Other non-DPA Commerce surveys and assessments on semiconductors in recent years have also identified certain shortfalls. For instance, with regard to printed circuit boards (PCBs), a 2022 BIS assessment found that only one U.S. firm is in the top ten global producers, with the remainder located in Japan and the PRC. Semiconductors and other components do not operate until they are assembled onto a PCB. PCBs are in all information and communication technology hardware, including in telecommunications hardware and end-user devices, and are also widely used in many other sectors, such as automotive, defense, and medical technology. In the past 20 years, the PRC has overtaken the United States as the global leader in PCB manufacturing and sales. The small PCB industry left in the United States leads in quality and performance, but lacks efficiencies created by automation technologies. While the 2022 BIS assessment did not rely on data collected pursuant to DPA authorities, recent interim results from DPA data collections around related semiconductor efforts confirm similar supply chain vulnerabilities.

4. Does business confidentiality under any statute affect your ability to share information with Congress? If so, please cite the relevant statutes that limit your ability to share information with Congress.

Response:

Section 1761(h) of the Export Control Reform Act of 2018 (50 U.S.C. 4820(h)) requires BIS to receive a request from a chair or ranking member of a Congressional committee or subcommittee of appropriate jurisdiction to provide information in connection with licenses and license applications for exports of items under Commerce jurisdiction.

Results from our industrial base assessments are governed by Section 705(d) of the DPA (50 U.S.C. 4555(d)). All responses to DPA surveys are treated as confidential. DPA survey information may be shared only in limited circumstances, with restrictions, and only if the Undersecretary for Industry and Security, the Secretary of Commerce, or the President determines that withholding the information is contrary to the national defense.

Certain provisions of the Defense Production Act are scheduled to expire on September 30, 2025. The Department of Commerce is eager to work with Congress to reauthorize the non-permanent provisions of the Defense Production Act. BIS will continue to assist Congress to ensure they have access to the necessary information.

5. In April, the Federal Reserve Bank of New York found that US export controls cost American suppliers a total of \$130 billion in market capitalization and additionally led to a drop in bank lending, profitability, and employment.
- a. What is your response to this study?
 - b. Do you believe these figures are accurate?
 - c. Does Commerce evaluate the potential economic impact of an export control decision before implementing?
 - i. If so, how?
 - ii. If not, how is this lack of calculus consistent with the first statement of policy in the Export Control Reform Act, *“The following is the policy of the United States: (1) To use export controls only after full consideration of the impact on the economy of the United States and only to the extent necessary”*?

Response:

The Federal Reserve study provided helpful anecdotes regarding the economic impact of U.S. export controls, but placed significantly more emphasis on the economic costs than the national security gains that came about as a result of U.S. export controls. It is also noteworthy that much of the report’s findings are based on non-random sampling of PRC companies that were specifically targeted due to national security and/or foreign policy concerns, meaning that the final results are not broadly generalizable.

In addition to open-source material, BIS utilizes available proprietary and classified information in coordination with interagency partners, the Intelligence Community, and U.S. and international law enforcement community to determine the impact that U.S. export controls have on American manufacturers and suppliers. We narrowly tailor our rules to specifically address our mission to “advance U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership.” Consistent with the Export Control Reform Act (ECRA) of 2018, we consider economic impact and engage directly with industry in developing and implementing export controls.

6. Semiconductor equipment manufacturers may have cut up to 2,000 jobs in Ohio due to foreign backfilling resulting from unilateral controls. Additional controls could cost jobs in Montana, Michigan, and Texas.
- a. Have reports of damage to U.S. jobs from past export control applications factored into your export control decisions?
 - i. If so, how?

ii. If not, why not?

b. Is this consistent with the guiding principles under the Export Control Reform Act?

Response:

Multilateral cooperation is vital to the success of export controls to protect our national security, and foreign backfilling as a result is counterproductive and hurts our economy. BIS understands that acting unilaterally generally minimizes the effectiveness of our controls and creates an unlevel playing field for U.S. companies, thereby potentially undermining U.S. technological leadership. History has shown that the U.S. must lead when our national security is at stake; at the same time, this Administration places the highest priority on working with our allies and partners to make sure that we act multilaterally or plurilaterally whenever possible.

BIS is in constant communication with international allies and partners that share our democratic values, security, and other interests. In order to enlist their assistance in aligning controls, we have worked closely with governments to share information on the current threat environment and discuss our approach to export controls. With respect to controls on semiconductor manufacturing equipment and related items, BIS implemented strict controls on the PRC in October 2022 and updated those controls in October 2023. Both Japan and the Netherlands imposed similar restrictions under their own laws.

To address foreign backfilling from our strategic competitors, BIS updates export controls to adjust to current trends and concerns. For example, in February 2023, BIS added nearly ten entities, including five in the PRC, to the Entity List for engaging in backfill activities in support of Russia's defense sector. These listings prohibit the targeted companies from purchasing items, whether made in the U.S. or with U.S. technology abroad. BIS will continue to guard against noncompliance with our export control rules.

BIS regularly assesses the impact of export control regulations on the U.S. economy, utilizing available open-source, proprietary, and classified information in coordination with the Intelligence Community and Department of Commerce and interagency colleagues, as well as the U.S. and international law enforcement community. These learnings contribute to BIS's rulemaking efforts, including updates to existing rules.

7. Have your department's semiconductor controls on China's semiconductor industry been successful?

a. How do you measure success on your controls?

Response

Our focus is on ensuring the PRC cannot use U.S. semiconductor technology for its military modernization. BIS's export controls on semiconductor equipment have limited the PRC's capacity at the 7nm node, which is six years behind the leading-edge technologies. While Huawei has developed the Ascend 910B, it has encountered significant difficulties expanding its production of that chip due to insufficient semiconductor chip yields at indigenous PRC fabrication plants (aka fabs). The use of legacy tools to produce 7nm chips requires more production steps, which increases costs and failure rates. Public reporting, based on industry sources, indicate low production yields, with some stating it is only in the 20% range as 4 out of 5 chips have defects.

For the most advanced chipmaking tools, BIS restricts exports to any actor in the PRC. However, such broad restrictions require multilateral applications with other technology producing countries to enhance effectiveness. For example, if the United States bans a certain deposition tool on a country-wide basis, but a substitute is available from a third country, then a U.S. country-wide ban will be ineffective and will reduce the long-term technology leadership of the United States. BIS is constantly calibrating which tools are most effective based on continuous monitoring of PRC activities, technological developments in chipmaking and tooling, and engagement with partner countries, who are also major tool suppliers.

In order to measure the effectiveness of export controls, BIS collects and analyzes relevant trade and export data, industry information (e.g., corporate ownership, parent/subsidiary locations), supply chain illumination data, and intelligence reporting. These key data sources enable BIS to answer key questions, such as what goods are being exported, to whom the goods are exported, and whether the ultimate consignee has received significant funding from potential adversarial sources. This also allows BIS to better identify transactions at high risk of transshipment or in violation of the EAR that would merit referral to our colleagues in Export Enforcement.

8. Please provide specific examples of export control actions during your time at the Bureau of Industry and Security, where your actions have led to friendshoring away from China.

Response:

As the operating environment becomes more challenging in the PRC, U.S. and multinational companies are seeking new locations for their technology operations. As a result of BIS's export control actions that restrict technology exports to the PRC yet facilitate exports to allies and partners, friendshoring is an indirect benefit. We published rules to this end

including an interim final rule that lessens license requirements for AUKUS partners² and a proposed rule to enhance License Exception Strategic Trade Authorization.³

9. Are you worried that your export controls are leading to indigenization of the Chinese semiconductor industry?
 - a. How are you tracking Chinese indigenization?
 - b. What steps can the U.S. take to prevent Chinese indigenization?
 - c. Have you seen any indication of China stockpiling semiconductor equipment? If so, please describe.

Response:

BIS takes seriously the issue of PRC indigenization of advanced-node semiconductor manufacturing equipment capabilities critical for the development and production of the next generation of advanced weapon systems, as well as critical and emerging technologies used in military applications. BIS closely monitors the development of PRC advanced-node semiconductor manufacturing capabilities not only at the facility/fab level, but also along the entire value chain, from startups seeking to design AI accelerator chips, to equipment manufacturers and their component suppliers, to companies producing additional inputs like software and materials. BIS relies on a number of tools, including public and non-public sources, to assess the state of PRC indigenization efforts. These tools include official PRC government documents, information obtained from industry, and other open-source intelligence, as well as classified information from the U.S. Intelligence Community.

For decades now, the PRC has been working to indigenize critical technology sectors to grow domestic capacity, as directed by the highest echelons of the Chinese government and Chinese Communist Party (CCP). Many of Beijing's efforts predate the bulk of our semiconductor and semiconductor manufacturing equipment (SME) export controls. That being said, BIS is focused on assessing foreign availability and the impact of BIS controls as part of our internal process for developing new export control policies, and part of this includes analyzing if/how our controls could incentivize new or faster innovation in a given targeted sector. This is an important part of our calculations in choosing when and how to implement new controls; BIS will always prioritize acting when U.S. national security or foreign policy interests are at stake.

To date, BIS has imposed controls on items that could be used to develop or produce indigenous semiconductor manufacturing equipment in the PRC. Our goal is to prevent the

² Export Control Revisions for Australia, United Kingdom, United States (AUKUS) Enhanced Trilateral Security Partnership, Correction, 89 Fed. Reg. 38837 (May 8, 2024), <https://www.federalregister.gov/documents/2024/05/08/2024-10079/export-control-revisions-for-australia-united-kingdom-united-states-aukus-enhanced-trilateral>.

³ Proposed Enhancements and Simplification of License Exception Strategic Trade Authorization (STA), 88 Fed. Reg. 85734 (Dec. 8, 2023), <https://www.federalregister.gov/documents/2023/12/08/2023-26681/proposed-enhancements-and-simplification-of-license-exception-strategic-trade-authorization-sta>.

PRC from developing sensitive technologies or products that are critical to the next generation of military, intelligence, surveillance, or cyber-enabled capabilities.

For the most advanced chipmaking tools, BIS restricts exports to any actor within the PRC. However, such broad restrictions require multilateral coordination with other technology producing countries. For example, if the United States bans a certain deposition tool on a country-wide basis, but a substitute is available from a foreign firm, then a country-wide ban will be ineffective, while reducing the long-term competitiveness of U.S. firms. BIS regularly calibrates which tools are most effective based on ongoing monitoring of PRC activities, technological developments in chipmaking and tooling, and engagement with partner countries, who are also major tool suppliers.

BIS is also aware of several recent media reports claiming that the PRC is stockpiling SME. We are monitoring this situation closely and speaking as necessary to relevant foreign governments and firms.

10. There are reports that China is attempting to “deAmericanize” its high-tech industry supply chains. Have you noticed this pattern of activity in spaces other than the semiconductor industry?

Response:

Reports indicate that the PRC has prioritized domestic substitution in all critical and emerging technologies ranging from information and communication technology, and artificial intelligence to space.

The PRC is working hard to be self-sufficient in all industries, not just semiconductors. We are focused on the long-term goal of limiting PRC military modernization, which is why we are constantly in talks with foreign governments and growing our multilateral coordination to address the threat the PRC’s technology and military modernization poses for global security.

11. Can you please describe the state of multilateral engagements with Japan, the Netherlands, and South Korea to advance their export control regimes?

- a. What steps are you taking to ensure a level field for U.S. firms?

Response:

Multilateral coordination is crucial to the effectiveness of export controls. We are building and strengthening export control relationships as circumstances dictate – through multilateral, bilateral, and plurilateral relationships. For example, the United States and 38 allies and partners of the Global Export Control Coalition (including Japan, the Netherlands, and South Korea) are imposing and enforcing substantially similar controls on Russia. The Dutch and Japanese imposed their own restrictions on semiconductor manufacturing

equipment to the PRC, comparable with our rules. BIS collaborates with Japan, the Netherlands, South Korea, and many others on outreach to other countries, such as those in Southeast Asia, to bolster capacity-building efforts related to export control administration and enforcement authorities and capabilities.

12. Have you seen any incidents of foreign nations backfilling U.S. market share following U.S. applications of unilateral export controls? If so, please provide all examples.
- a. Would you agree that a foreign nation backfilling a U.S. product negates the effect of a U.S. export control while damaging the domestic U.S. economy?
 - b. There are widespread reports of foreign backfilling in the semiconductor industry. What efforts are you taking to address the backfilling and what impact has this backfilling had on U.S. national security?

Response:

BIS is aware of cases of foreign nations backfilling U.S. products after the implementation of unilateral controls.

While BIS prefers to implement multilateral controls, multilateral and unilateral actions are both necessary. Imposing unilateral controls when other key supplier countries do not can be akin to “damming half the river,” which can fail to fully protect our national security interests or advance U.S. technological leadership.

However, there are some cases where the United States is sufficiently predominant in production of a critical technology to the extent that unilateral controls can be effective. For example, controls on advanced AI chips have imposed significant constraints on the PRC’s ability to train large language models. The PRC’s closest competitor, Huawei’s Ascend 910B, lags in performance. These challenges make both AI training and inference for Chinese companies more expensive and less efficient and potentially hinder the deployment of AI models at scale.

BIS is diligently working to multilateralize controls through constant engagement with our allies and partners. Coordinated controls reduce instances of evasion or backfill by other suppliers from other countries, ensuring that our controls remain effective over the long term.

13. Under your tenure at the Bureau of Industry and Security, how many times have you applied the Foreign Direct Product Rule?

- a. Does each additional use of the Foreign Direct Product Rule limit private sector firm's ability to ensure compliance with the ever-increasing amount of rule applications?

Response:

BIS has added six Foreign Direct Product Rules (FDPRs) during my tenure as Assistant Secretary. In February 2022, in response to Russia's invasion of Ukraine, BIS added two new FDPRs specific to all of Russia and Belarus and to Russian and Belarussian military end users. Thereafter, BIS published the advanced-computing and supercomputer and Iran FDPRs, as well as an additional Entity List FDPR. In each of the instances, we addressed an acute national security concern.

The FDPRs are identified in Section 734.9 of the EAR, each of which identifies the product scope and destination, end-use, or end-user scope for which the restrictions would apply, including to certain parties on the Entity List or designated as "Russian/Belarussian Military End Users," under sections 734.9 (e) and (g).

Export Administration and our Export Enforcement colleagues work hard to ensure that U.S. exporters and broader industry understand the rules and their compliance obligations through seminars, public events, direct engagement with exporters who have questions through our Office of Exporter Services, formal advisory opinions, and other engagements. Effective compliance by industry is the frontline of export controls, and we provide extensive assistance with compliance efforts.

14. You recently publicly stated that your interim final firearms rule received 13,000 public comments.
 - a. Why are the comments currently not publicly available on the Federal Register website?
 - b. Does BIS plan to review each comment and address them?
 - c. How does BIS plan to review and respond to the relevant comments?

Response:

BIS accepted public comments on this rulemaking through July 1, 2024, of which we received roughly 13,000 public comments. Comments on the EAR and other BIS regulations are reviewed and posted by a select handful of BIS staff. It takes time to post each comment. As of September 30, 2024, more than 10,000 comments have been posted to Regulations.gov.

Reviewing the comments and determining an appropriate response takes time. BIS intends to identify key issues raised in public comments, and update industry outreach and guidance as appropriate.

15. In a July 24, 2024, response to my May 21, 2024, letter, the Commerce Department stated that “Exports to non-governmental end users in the high-risk destinations listed above historically represent about seven percent of total exports of firearms and related items under BIS jurisdiction, or about \$40 million annually.”
 - a. Please explain how you reached this \$40 million figure.
 - b. Please provide the total number of licenses revoked in accordance with the IFR.
 - c. Please provide the total value of authorized exports licenses that were revoked by this IFR and the total value remaining open of licenses as of the date of revocation.

Response:

The State Department has identified certain destinations in which there is a substantial risk that firearms and related items sold to non-government end users will be diverted or misused in a manner contrary to U.S. national security and foreign policy. Those destinations are listed in Supplement No. 3 to Part 742 of the EAR (“High-Risk Destinations for Firearms and Related Items”). Historically, the non-governmental end users in the 36 destinations identified have received about \$40 million annually in exports of firearms and related items subject to BIS jurisdiction.

To reach this figure, BIS reviewed export data from the Automated Export System shipped under a BIS license for items classified under ECCNs 0A501, 0A502, 0A504, and 0A505 to all countries and end users from 2020-2023. BIS found that on average, \$600 million was shipped worldwide under a BIS license. BIS then reviewed all shipments destined to any end user in one of the 36 destinations, undertaking a manual review of the end-users identified on the licenses recorded on each shipment to determine whether the items were destined to government or non-government parties. BIS found that on average between 2020-2023, exports of 0A501, 0A502, 0A504, and 0A505 items to non-government end users in these 36 destinations amounted to approximately \$40 million per year, or approximately 7% of total (\$600 million) exports under a BIS license for these items.

Based on an extensive policy review in collaboration with interagency partners, BIS determined that the exports authorized by these licenses (all involving non-government end users) pose substantial risks to national security and foreign policy and must be reviewed under a presumption of denial.

On July 1, 2024, BIS revoked approximately 1,300 active licenses validated between 2020 and 2023 that authorized shipments to non-government end users in the 36 destinations because those licenses had not been reviewed under the updated policy that applies to such

exports. Accordingly, continued exports under those licenses could create a substantial risk of diversion or misuse in a manner contrary to U.S. national security and foreign policy. The companies impacted by these revocations were provided advance notice on April 30, 2024, that certain of their licenses were set to be revoked. In addition to specifying which license(s) will be revoked, instructions on how to contact BIS were included in the notification letter. Anyone can reapply under BIS's new licensing review policy, and their application will be reviewed without prejudice.

For licenses issued prior to the IFR, there was generally no purchase order required to support the total value on the license. Exporters had shipped approximately \$125 million worth of firearms and related items under these licenses before the licenses were revoked on July 1, 2024. Close to 400 of these licenses, the majority of which were approved in 2020-2022, had a 0% utilization rate at the time of revocation.

The exporters impacted by the rule's revocations continue to hold approximately \$22 billion in valid licenses (almost 15,000 total licenses) that were not impacted by the revocations. As of September 30, 2024, approximately \$31 billion is authorized under current, unexpired firearm licenses regardless of destination.

16. A July 24, 2024, response to my May 21, 2024, letter, stated that "the Department considered the impact on U.S. commercial, economic, national security, and foreign policy interests when crafting the firearms IFR." How much weight did the commercial and economic impact carry relative to other considerations?

Response:

First and foremost, BIS's actions are aimed at safeguarding U.S. national security and foreign policy interests. As with every rule, we consider the economic impact alongside the national security and foreign policy interests. The rule is narrowly tailored to identify and restrict firearm exports that threaten U.S. national security and foreign policy, while allowing exports of firearms that do not.

17. In a July 24, 2024, response to my May 21, 2024, letter, the Department stated that you "engaged with ... foreign allies and partners..."
- a. Which foreign allies and partners did the Department engage with?
 - b. What method of engagement did the Department use with each foreign ally and partner?
 - c. Are any allies and partners engaging in similar export restrictions?

Response:

As described in the rule, BIS coordinated bilateral talks with foreign governments during its review of its licensing policy. Specifically, BIS spoke directly with officials in countries who manufacture firearms, such as the United Kingdom, Germany, and Austria, and outreached to other European allies including France and Italy. In particular, during BIS's engagement with Austria, BIS learned that on November 15, 2023, Austria paused the approval of new export licenses after uncovering instances of diversion of Austrian-made firearms. Austrian officials indicated that they were undertaking a review to determine the cause of the diversion and assessing potential legal changes to counter future diversion. We also conducted bilateral discussions with Ecuador and Peru to discuss issues around diversion and BIS licensing policy.

In addition to those bilateral engagements, partner governments, particularly in the Western Hemisphere, have expressed concern that U.S. firearms are fueling violence, criminal activity, and instability in their countries. For example, BIS's Export Enforcement engages consistently with partner governments in the Caribbean Community (CARICOM) to discuss firearms trafficking and diversion concerns. Based on these engagements and more, we carefully reviewed and updated our policy to increase scrutiny of firearms exports to make sure they don't get into the wrong hands, while allowing exports of firearms that don't threaten national security or foreign policy interests. The vast majority of firearms exports are to partners and allies, and the rule will not substantially impact these destinations.

In addition, our partners in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technology (Country Group A:1) have demonstrated a similar commitment to countering diversion and misuse of firearms and related items, advancing human rights, and promoting mutual security. In fact, the European Commission (EC) just made significant changes to their policies on firearms exports to limit risks of diversion and misuse of such items, and will enhance security and address firearms trafficking. The EC's revised rules include clear and common procedures for the import, export and transit of firearms for civilian use, as well as simplified procedures for hunters, sport shooters, historical reenactors and exhibitors.

18. In a July 24, 2024, response to my May 21, 2024, letter the Department stated that the 36 countries selected "...present a substantial risk of firearm diversion or misuse adverse to U.S. national security and foreign policy."

- a. Of the 36 countries selected, how many of these countries does the U.S. have agreements or treaties with to support activities in their respective countries?

Response:

To support Commerce's ongoing efforts to impose export controls that further U.S. national security and foreign policy, State has developed a list of destinations in which there is a substantial risk that lawfully exported firearms sold to non-governmental end users could be diverted or misused in a manner adverse to U.S. national security and foreign policy. For each

country on the list, the State Department looked at a holistic set of factors, including firearms trafficking or diversion, terrorism, corruption, human rights concerns and political violence, state fragility, organized crime or gang-related activity, and drug trafficking. State gathered data, case studies, and other evidence relevant to assessing how each of those factors apply in each country. State also consulted with U.S. embassy officials, including those with experience working with local law enforcement agencies, subject matter experts and regional experts, and other federal agencies.

The list reflects a comprehensive analysis of where lawful exports of firearms and related items to non-government end users pose substantial risks or diversion or misuse in a manner contrary to U.S. national security and foreign policy interests. As noted in the State memo, "U.S. Embassy officials with country-specific expertise were able to provide important on-the-ground context that could not be gleaned from other data sources. Such insights included ... the volume and nature of bilateral trade ... and diplomatic sensitivities, including implications for collaboration with law enforcement and other foreign policy priorities."

19. In a July 24, 2024, response to my May 21, 2024, letter, the Department cited an "...an increased risk that the diversion or misuse of firearms and related items will increase the ability of cartels, gangs, and other criminal organizations to undermine U.S. national security and foreign policy," regarding the 36 countries designated as "high risk." Does the Department believe that this warrants a "presumption of denial," even if the Department does not provide individual facts to support this assertion?

Response:

For each country on the list, the State Department looked at a holistic set of factors, including firearms trafficking or diversion, terrorism, corruption, human rights concerns and political violence, state fragility, organized crime or gang-related activity, and drug trafficking. State gathered data, case studies, and other evidence relevant to assessing how each of those factors apply in each country, and it consulted U.S. embassy officials with on-the-ground knowledge of conditions in those countries. The list reflects a comprehensive analysis of where lawful exports of firearms and related items to non-government end users pose substantial risks or diversion or misuse in a manner contrary to U.S. national security and foreign policy interests.

Applying a presumption of denial to license applications for those exports will ensure that the licensing process fully and consistently accounts for national security and foreign risks in destinations of concern. Transparency with respect to destinations of concern will also promote predictable and timely review of license applications and will help industry and other stakeholders understand the licensing process.

In addition, a presumption of denial, as opposed to an absolute prohibition, provides BIS with the flexibility to tailor its review to the individual facts and related policy interests.

Exporters have the opportunity to overcome the presumption of denial by demonstrating that a specific transaction does not present a substantial risk of diversion or misuse.

20. The Bureau of Alcohol, Tobacco, Firearms & Explosives' (ATF) report on international crime guns states that recovered and traced crime guns represent less than 1% of the total firearms lawfully exported out of the U.S. Does BIS concur with this assessment?
- a. If yes, why has BIS implemented a policy of presumption of denial for 36 countries which is not supported by the ATF report?
 - b. If no, please explain why BIS does not accept the ATF data, which is supported by verified information.

Response:

BIS approaches export controls on firearms and related items under our jurisdiction with the primary objective of protecting U.S. national security and foreign policy interests. In developing the changes implemented by the Firearms Rule, BIS considered reports and analyses on the diversion and misuse of lawfully exported firearms. BIS worked together with interagency export control partners in the Departments of Defense, Energy, and State, as well as other federal agencies with technical expertise in firearms and related items.

The 2023 National Firearms Commerce and Trafficking Assessment provides data regarding the diversion of lawfully exported firearms. As described in that report, participating law enforcement agencies in foreign countries can submit firearm trace requests to ATF's eTrace system to help determine the purchase or ownership history of a recovered crime gun. ATF's analysis of all international crime gun trace requests received between 2017 and 2021 indicates that at least 11% (18,749) of traced firearms were lawfully exported from the United States and later recovered in a foreign country. For countries outside of North America, at least 37% of firearms submitted to ATF were lawful exports; for countries in Central America, at least 19% of firearms submitted to ATF were lawful exports. These data are of particular concern given that ATF was working with a limited set of international crime guns for which a trace request was submitted. This report and the other data referenced in the rule indicate that a sizeable portion of international crime guns are diverted from lawful exports.

Moreover, through our review process, BIS identified specific instances in which lawfully exported firearms were diverted in a manner that threatens our national security and foreign policy objectives. In one case, a firearm that had been licensed for export to one country was subsequently diverted to a bordering country and used in a political assassination. BIS also identified instances of licensed firearms and ammunition exports being diverted to Russia via commercial resellers in third countries.

In addition, partner governments, particularly those in the Western Hemisphere, have expressed concern that U.S. firearms are fueling violence, criminal activity, and instability within their countries. Based on all this evidence, we carefully reviewed and updated our policy to increase scrutiny of firearms exports to make sure they don't get into the wrong hands, while allowing exports of firearms that don't threaten national security or foreign policy interests. The vast majority of firearms exports are to partners and allies, and the rule will not impact these destinations. In other words, this rule is narrowly tailored to address risks to national security and foreign policy.

21. Since the May 30 effective date of the new firearms rule, how many license applications for firearms and related items (e.g., optics, shotguns, ammunition) has BIS received?
- a. What is the average number of continuous calendar days, counted from the date of submission until the date of issuance, for approval of an export license?
 - b. During this same period, what is the number of license applications “Returned Without Action” and how does this compare to applications processed during the same time period in 2023?
 - c. Does BIS anticipate a major increase in the number of required licenses, and a corresponding need for an increase in BIS funding and staffing levels, in order to meet the need and implement the interim final rule?
 - d. Why does the BIS interim final rule require license applications to include purchase orders or separate purchase orders that are not required under current regulations for any other commodity, including military commodities transferred from the U.S. Munitions List?
 - e. How many total licenses has BIS revoked since the finalization of Export Control Reform?

Response:

As of September 9, 2024, 1,634 license applications for firearms and related items had been processed and validated (approved, denied, or returned without action) since the firearms rule went into effect on May 30, 2024.

Applications for firearms and related items submitted since May 30, 2024, currently have a median total processing time of 32 days, which is almost a week faster than the average processing time for all BIS licenses in 2023, which was 38 days. Applications for end users in Country Group A:1 have been processed even faster, with a median processing time of 28 days. Applications for exports to end users in the 36 countries that the Department of State determined present a substantial risk of firearm diversion or misuse adverse to U.S. national security and foreign policy (as listed in Supp. No. 3 to part 742 of the EAR), as well as applications for end users in Country Group D:5 (U.S. Arms Embargoed Countries), have taken longer to review, with median processing times of 36 days and 51 days, respectively. These longer processing times for High Risk and D:5 countries are consistent with BIS’s and the interagency’s efforts to carefully scrutinize transactions for national security and foreign policy concerns, including the risk of diversion to or misuse by foreign criminal organizations and other malign actors.

As exporters begin to adjust to the firearms rule’s new requirements and review policies and BIS continues to provide clarify expectations and communicate consistent guidance on how exporters should comply with the new requirements, processing times may decrease.

From May 30, 2024, through August 31, 2024, 169 newly submitted license applications were Returned Without Action (RWA). These 169 RWAs between May 30, 2024, and September 3, 2024, is a higher rate of RWAs than the previous year's period (May 30, 2023 – August 31, 2023) of 64. A higher rate of RWA is expected when implementing a new rule, as exporters adjust to the new documentation requirements or export control classification numbers.

Prior to the effective date of the Firearms Rule on May 30, 2024, BIS identified a subset of pending license applications that were submitted prior to the release of the rule, and thus did not meet the new requirements outlined in the rule. BIS returned without action these 1,066 pending license applications because they could not have been processed and approved in accordance with the new requirements. Exporters were notified if their applications were Returned Without Action, and were provided with guidance on the new requirements and best practices for resubmitting applications. Applications may also be returned without action for other reasons, including informing the exporter that a license is not required or that a license exception may apply to their transaction. Also, if there is a request for information from another agency and the exporter is not able to provide the information in a timely manner, the application is returned without action and the exporter is encouraged to reapply when they have this information.

BIS does not expect this rule to be burdensome to license applicants or to BIS staff. Several of the measures we adopted in the new rule may speed license application review. For example, as exporters are providing documentation with the license application submission, this will limit the need for certain back-and-forth after the application is filed. BIS also formalized in the Export Administration Regulations an interagency group on firearms export license review that is comprised of the Departments of Commerce, Defense, Energy, and State, who chairs the group. This group supplements and does not supplant the usual export licensing review process. This group has helped to streamline the interagency's review of applications by promoting interagency discussion of overall firearms licensing policy concerning high-risk countries and resolving differences that have emerged during agency review of individual license applications.

BIS has not seen a marked increase in license application submissions since the Firearms Rule went into effect on May 30, 2024. Exporters submitted fewer applications in June and July 2024 than they submitted in June and July over the previous four years during which BIS licensed these items (2020, 2021, 2022, 2023). The average submissions each month between 2020-2024 was 652. In June 2024, 531 applications were submitted, and in July 2024, 416 applications were submitted, for a 2024 average of 474 license application submissions each month.

The IFR amended the EAR to require that a purchase order be submitted for exports and reexports of firearms and related items to non-A:1 countries. Previously, exporters were not required to submit a purchase order with BIS license applications, unless requested during the course of BIS's review of a particular application. This practice created a number of challenges. First, BIS processed and reviewed many applications that did not result in actual exports, thereby unnecessarily expending staffing resources. Previously, less than 20% of licensed quantities were actually exported. In addition, such licensing that did not result in exports offered limited visibility into actual demand for U.S. firearms abroad, which in turn made effective monitoring of diversion risks more difficult. Requiring purchase orders for exports and reexports to non-A:1

countries will enable BIS to use licensed quantities to estimate *bona fide* local demand, thereby ensuring that BIS can appropriately evaluate the national security and foreign policy risks associated with a given transaction and effectively allocate review and processing resources.

Since the transfer of firearms and related items to the BIS on March 9, 2020, BIS has revoked 2,569 total licenses for any item under BIS jurisdiction.

22. Please explain how our national security will be impacted when the demand for firearms in the 36 listed countries will be met by sellers outside of the United States.

Response:

BIS reiterates its commitment to combatting the diversion and misuse of U.S. firearms by bad actors across the world, while allowing the export of firearms to end users who do not present national security or foreign policy risks. We will not engage in a race to the bottom with Russia and the PRC to sell U.S. firearms to criminals and cartels.

23. Have you consulted with Israeli government officials, including embassy officials, since implementation of the IFR to ensure that unnecessary, dangerous delays in the granting of licenses was not occurring?

- a. Which specific individuals did BIS consult with from the Israeli government and on what dates?
- b. Does BIS believe that Israeli's have a human right to self-defense?
- c. Does BIS believe that Israeli civilians should be legitimately concerned about terrorist attacks similar to what occurred on October 7, 2023?

Response:

The U.S. commitment to the defense of Israel is ironclad, and the U.S. government will continue to support Israel's ability to defend itself. The Department of Commerce has been in close consultation with the appropriate Israeli government entities on the quantities of exports requested and the documentation required for import to Israel. In particular, BIS has engaged with representatives of the Israeli Ministry of Defense, the Ministry of National Security, and the Trade & Economic Mission at the Embassy of Israel. As with all license applications seeking to export or reexport firearms, ammunition, and related items, applications seeking to export or reexport those items to Israel are reviewed to determine whether the transaction poses risks to national security and foreign policy interests, including human rights (see sections 742.6(b) and 742.7(b) of the Export Administration Regulations). BIS is evaluating all license applications through the standard interagency process, which includes consultation with the Departments of State and Defense, with careful review on the end-users and in consideration of the end-use and security environment.

24. Does BIS believe that the lawful export of firearm products to vetted, longstanding customers in foreign countries and with the approval of that foreign country's government, cause or contribute to gun-related crimes or political instability?

a. If yes, what evidence does BIS rely on to come to this conclusion?

Response:

BIS is committed to combatting the diversion and misuse of U.S. firearms by bad actors abroad, while allowing the export of firearms to end users who do not present national security or foreign policy risks. Those that do not present a risk may include longstanding customers in foreign countries that have approval of that foreign country's government to import U.S. firearms and related items. BIS always considers the licensing history (prior approvals or denials) for all parties involved in the transaction when reviewing applications, including for license applications seeking authorization to export U.S. firearms.

As discussed in the rule and above, BIS identified recent instances in which lawfully exported firearms were diverted or misused in a manner that threatens our national security and foreign policy objectives. BIS identified specific instances in which lawfully exported firearms were diverted in a manner that threatens our national security and foreign policy objectives. In one case, a firearm that had been licensed for export to one country was subsequently diverted to a bordering country and used in a political assassination. BIS also identified instances of licensed firearms and ammunition exports being diverted to Russia via commercial resellers in third countries; such firearms and ammunition may be used to support Russia's further invasion of Ukraine. BIS also considered reports and analyses on the diversion and misuse of lawfully exported firearms.

BIS also reviewed aggregate data showing that a substantial number of firearms recovered by foreign law enforcement agencies were lawfully exported from the United States. Additionally, partner governments, particularly those in the Western Hemisphere, expressed concern over the diversion and misuse of lawfully exported U.S.-made firearms in their countries that were fueling regional instability, human rights violations, and political violence.

25. According to the Export Control Reform Act, "*Export controls applied unilaterally to items widely available from foreign sources generally are less effective in preventing end-users from acquiring those items. Application of unilateral export controls should be limited for purposes of protecting specific United States national security and foreign policy interests.*" As it relates to BIS's latest actions, are you aware of any other countries having similar export controls like the ones your department implemented, particularly the new licensing requirements for sporting shotguns and firearm scopes?

a. If so, which countries?

- b. How have the export controls instituted by BIS supported our national security and foreign policy interests?

Response:

As described in the rule, BIS coordinated bilateral talks with many foreign governments during its review of its licensing policy. During BIS's engagement with Austria, BIS learned that on November 15, 2023, Austria paused the approval of new export licenses after uncovering instances of diversion of Austrian-made firearms. Austrian officials indicated that they were undertaking a review to determine the cause of the diversion and assessing potential legal changes to counter future diversion, after which the pause would be lifted. In addition, the European Commission just made significant changes to their policies on firearms exports to limit risks of diversion and misuse of such items.

Many other supplier countries have similar standards for reviewing firearms exports. EU countries apply common principles such as assessing human rights, internal stability, and armed conflict in the destination country, as well as risk of diversion. Over 100 countries are party to the Arms Trade Treaty (ATT), including the PRC. The ATT requires states party to consider whether exports of small arms and light weapons could be used to commit or facilitate a serious violation of international human rights, undermine peace and security, or be used for terrorism or organized crime. Likewise, many countries are partners in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technology (Country Group A:1). Governments in A:1 destinations have demonstrated a commitment to export controls as participants in the Wassenaar Arrangement and share our interest in countering diversion or misuse of firearms and related items, advancing human rights, and promoting mutual security.

The Firearms Rule added license requirements for certain items, like select firearms scopes and shotguns, on the Commerce Control List when destined to countries and/or end users that previously did not require a license. For example, prior to the rule, shotguns were subject to different controls under ECCN 0A502 based on the barrel length and particular end user (specifically, police or law enforcement). However, these items have long been subject to the Export Administration Regulations, and many of the requirements in the rule were already in place for other countries, including our closest trading partner, Canada. The changes made in the IFR ensure consistency in how those regulations are applied, as well as reflecting the significant relationship of diversion and misuse of firearms and related items to U.S. foreign policy and national security objectives.

26. How many licenses did BIS place in "Hold Without Action" status which were not granted or acted upon as a result of the "90 day pause" that actually lasted 181 days?

Response:

On October 27, 2023, BIS placed certain license applications on Hold Without Action (HWA) status pursuant to the announced pause. Applications subject to the pause or HWA include all

non-governmental end users in destinations outside of Country Group A:1, Israel, and Ukraine. BIS's IT systems make it difficult to calculate the exact number of applications placed on HWA throughout the pause period. However, BIS estimates that approximately 1,200 license applications were placed on HWA status. This total reflects licenses that were submitted before October 27, 2023, or licenses that were submitted between October 27, 2023, through May 30, 2024, when the pause was lifted.

Over the course of the pause, BIS validated 1,884 licenses applications not covered under the pause (approved, denied, or returned without action). Of these, 1,492 licenses were approved worth approximately \$1.7 billion.

The pause was lifted on May 30, 2024, and no license applications for firearms or related items remain on HWA.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR SCOTT
FROM PAUL ROSEN**

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

Ranking Member Tim Scott

Question 1

Mr. Rosen, your core responsibility as Assistant Secretary of Investment Security is to ensure that U.S. national security is not compromised by malign foreign investment. We must stay vigilant as our adversaries attempt to find new and creative ways to compromise our national security. Can you describe the measures you evaluate when looking at the national security threat of an inbound CFIUS case?

Answer: The Committee on Foreign Investment in the United States (CFIUS) reviews every covered transaction that is before the Committee to determine the effects of the transaction on the national security of the United States. In any assessment, review, or investigation of a covered transaction, the Committee takes into consideration, as appropriate, the factors identified by Congress in section 721(f) of the Defense Production Act, as well as any additional factors identified by the President, including those in E.O. 14083 relating to supply chain resilience and security, technologies that are fundamental to U.S. technological leadership, incremental investments by a foreign person in specific sectors or technologies, cybersecurity risks, and concerns surrounding sensitive data.

Once a covered transaction is before the Committee, CFIUS can take action to mitigate any national security risk arising from the transaction. As prescribed by statute, such action must be based on a risk-based analysis, which considers three elements: 1) the threat, which is a function of the intent and capability of a foreign person to take action to impair the national security of the United States; 2) the vulnerabilities, which are the extent to which the nature of the U.S. business presents susceptibility to impairment of national security; and 3) the consequences to national security, which are the potential effects on national security that could reasonably result from the exploitation of the vulnerabilities by the threat actor.

a. *Does CFIUS screen for matters of national interest?*

Answer: CFIUS is mandated by statute to review transactions for national security risks.

b. *Does CFIUS consider domestic political interests when evaluating cases?*

Answer: Section 721 of the Defense Production Act sets forth a process which includes CFIUS undertaking a thorough, fact-specific analysis of potential national security risks arising from the transaction. As part of that process, CFIUS leverages expertise from across the government and focuses on risks to national security. Indeed, subject-matter

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

experts and career civil servants from across the Executive Branch conduct a robust analysis in every case. This analysis considers, as appropriate, the factors identified in section 721(f) of the Defense Production Act as well as those in E.O. 14083. This process allows the U.S. to maintain its open investment environment consistent with the protection of national security.

Question 2

I am worried that CFIUS is looking at cases in terms of military hard power or direct physical threat, like someone directly downloading sensitive weapons designs and taking them to a foreign nation. I am worried that CFIUS is missing some of the more important factors like long-term influence. How can CFIUS more effectively evaluate an investment’s foreign influence on a long-term basis?

Answer: As part of its risk-based analysis, CFIUS evaluates the threat that the foreign person involved in the transaction may take action to impair the national security of the United States. CFIUS considers both the foreign person’s intent and capability to take such action, including how the covered transaction would enhance the foreign person’s capability to act in the future. The President’s most recent Executive Order on CFIUS, E.O. 14083, includes among other things the importance of the Committee considering, as appropriate, whether a covered transaction could reasonably result in future advancements and applications in technology that could undermine U.S. national security. Additionally, the Committee considers the national security risks posed by a foreign person’s incremental investment in specific sectors or technologies, as well as the general share of foreign ownership in a particular sector of the economy. Such risks may include the long-term effect of foreign investment.

Question 3

Do you have any additional information that you can provide on public reports around the Tutor.com case, in which your Department reportedly signed off on a mitigation deal allowing a Chinese-aligned firm to acquire a controlling stake in an online teaching company that has a wide reach to our K-12 education system and U.S. service members?

a. In this case did you factor in the threat of Chinese influence on our education system?

Answer: See below.

b. How were you able to square this case with China’s national security law which allows the Chinese government to compel Chinese firms to share information?

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

Answer: CFIUS is subject to strict confidentiality as provided by statute, and, consistent with law and practice, I cannot publicly comment on whether a particular transaction was reviewed or is undergoing review. After consideration and completion of CFIUS’s review of a covered transaction, with all action being concluded, and consistent with its authorizing statute, CFIUS provides the Members of Congress specified in its authorizing statute with a summary of the transaction, and upon request, a classified briefing.

More generally, the Committee takes risks to national security very seriously, and reviews every covered transaction before CFIUS to determine the effects of the transaction on the national security of the United States. The Committee can take action to mitigate any risk to the national security of the United States that arises as a result of the covered transaction, and such action is based on a robust analysis of the threat, vulnerabilities, and consequences to national security related to the transaction.

Question 4

As sovereign wealth funds increase their equity positions in advanced future technologies, how is CFIUS working to ensure that sovereign purchases do not result in technology transfer?

Answer: In any covered transaction, including those involving sovereign wealth funds, CFIUS assesses *inter alia* how the acquiring entity might access or gain insight into or influence over the target U.S. business, including those with emerging technologies. For every covered transaction, CFIUS determines whether specific rights or access might result in a risk to national security.

In covered transactions where CFIUS determines that there is a risk relating to a foreign person’s access to some technology, it can take measures to mitigate such risk. The CFIUS Annual Report to Congress covering 2023 notes a few of these measures, such as the following: prohibiting or limiting the transfer or sharing of certain technical information; ensuring that only authorized persons have access to certain technology, systems, facilities, projects, or sensitive information; ensuring that computer networks are segregated; destroying sensitive information; and ensuring that certain facilities, equipment, and operations are located only in the United States.

To address a national security risk, CFIUS may also refer a transaction to the President, who has the sole authority under Section 721 of the Defense Production Act to suspend or prohibit a transaction.

a. How is CFIUS addressing potential third-nation coordination through direct party capital investments?

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

Answer: In any covered transaction before CFIUS, the Committee evaluates the foreign person’s ultimate beneficial ownership and ties to third countries. Pursuant to statute, the Director of National Intelligence provides the Committee with an analysis of any threat to the national security of the United States posed by any covered transaction.

If CFIUS determines that there is a risk to national security due to a foreign person’s ties to a third country, CFIUS can take action to address that risk through an enforceable agreement with the transaction parties or enforceable conditions imposed on the parties, including in the ways outlined in the response above and in the 2023 CFIUS Annual Report. CFIUS may also refer the transaction to the President. The President may suspend or prohibit the transaction, including by requiring divestment.

Question 5

Is CFIUS actively considering expanding its exempted foreign states, or whitelist, of nations?

Answer: The concept of an excepted foreign state (EFS) was first introduced in CFIUS’s regulations published in 2020 implementing the Foreign Investment Risk Review Modernization Act of 2018 (FIRREA). At that time, three countries were identified as EFS. In 2022, CFIUS made a determination with respect to a fourth country. We will continue to carefully consider whether to add additional countries, recognizing the application of the EFS concept carries potentially significant implications for the national security of the United States.

a. *What criteria would a currently non-exempted foreign state need to undertake for CFIUS to add them to exempted foreign state nation status?*

Answer: The Treasury Department has published on the CFIUS section of its website the factors that the Committee will take into consideration when making a determination regarding a foreign state’s process to review foreign investment for national security in its own country and its cooperation with the United States with respect to review of foreign investment. These factors focus on the substance of a foreign state’s process and cooperation with the United States to address national security risks arising from foreign investment, and do not prescribe a specific form. Note that these factors and the determinations are relevant only to the status of a foreign state as an EFS under CFIUS’s regulations.

Question 6

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

Mr. Rosen, I saw that CFIUS just undertook a large expansion of the real estate listings. Could you talk about the process, and why all of a sudden, a large number of entities were added?

Answer: The U.S. Department of Defense, a member of CFIUS, continuously assesses its military installations and the geographic scope established under the CFIUS real estate regulations to ensure appropriate application in light of national security considerations, which can evolve over time. The proposed rule, issued in July 2024, that would add over 50 military installations, across 30 states, to the existing list of installations around which CFIUS has jurisdiction is the result of a recent comprehensive assessment conducted by the Department of Defense. This assessment included coordination across all military services, considering factors such as the operations, assets, missions, and training at each installation and appropriateness for coverage under CFIUS’s authorities. A prior update was made to the CFIUS regulations in 2023 as a result of the assessment of military installations by the Department of Defense at that time.

a. *Do you believe that CFIUS should more regularly review its real estate listings?*

Answer: As noted in the final rule establishing CFIUS’s real estate regulations and as has been applied in practice, the Department of Defense regularly assesses its military installations to ensure appropriate coverage in light of national security considerations and consistent with the authority provided by statute. In 2020, Treasury published a list of installations around which CFIUS has jurisdiction for purposes of certain real estate transactions. In August 2023, Treasury, in coordination with the Department of Defense, added eight military installations to that list. Since then, the Department of Defense has completed a comprehensive assessment of its military installations, which resulted in the changes in the July 2024 proposed rule. The Treasury Department, in coordination with the Department of Defense and other members, will continue to ensure the sites listed are appropriate and responsive to national security concerns.

b. *Several high-profile CFIUS cases have been withdrawn and refiled many times. Does CFIUS have the authority it needs to stop malign foreign investments?*

Answer: Parties may withdraw a notice after acceptance by the Committee only if the Committee approves a written request for withdrawal from the parties. Over time, parties have requested withdrawals for a number of reasons. For example, in some cases in which the parties are unable to address all of the Committee’s outstanding national security concerns within the initial review phase or subsequent investigation period, the parties might request to withdraw and refile their notice to provide themselves with additional time to answer outstanding questions or to attempt to further negotiate a potential mitigation agreement, if appropriate. The number of withdrawals and refiles is

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

a function of the specific facts and circumstances of the particular transactions reviewed by the Committee. Given Treasury’s focus on efficiency, the withdraw and refile rate decreased in 2023 for the first time in several years.

- c. *Recently, the International Emergency Economic Powers Act has been legally challenged in U.S. courts. Are you confident that the pending rule associated with your Department’s NPRM relating to outbound investments would hold up to challenge in court?*

Answer: The President’s declaration of a national emergency in Executive Order 14105 is consistent with the emergency authorities granted to the President by the International Emergency Economic Powers Act (IEEPA). As noted in E.O. 14105, the President finds that advancement by countries of concern in sensitive technologies and products critical for the military, intelligence, surveillance, or cyber-enabled capabilities of such countries constitutes an unusual and extraordinary threat to the national security of the United States, which has its source in whole or substantial part outside the United States, and that certain United States outbound investments risk exacerbating this threat. The President declared a national emergency to deal with this threat. The rulemaking of the Treasury Department to implement E.O. 14105 is consistent with the authority provided to the President by IEEPA.

- i. *Would a court challenge to the International Emergency Economic Powers Act pose any potential challenge to existing U.S. sanctions programs?*

Answer: As has been the case for decades, most U.S. sanctions programs are established and administered pursuant to the emergency authorities granted to the President by IEEPA and the National Emergencies Act. While the potential impact of a court challenge to IEEPA itself or sanctions programs promulgated thereunder would ultimately depend on the specifics of the case, the Treasury Department has a long history of effectively administering and enforcing U.S. sanctions programs consistent with IEEPA and other applicable authorities.

Answer 7

Please provide a rough estimate of the number of individuals and the amount of time from employees of the Treasury Department that went into the development of President Biden’s Executive Order on Outbound Investments and the related Notice of Proposed Rulemaking.

Answer: As with other executive orders, the Treasury Department, along with other interagency members, worked together in supporting the President’s Executive Order 14105, including engagement with U.S. allies and partners and industry stakeholders on the objectives of the program, drafting the related rulemakings, and consideration of

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

public input through the rulemaking process. While I don't have precise figures to share, implementation thus far has included work across the Treasury Department and the interagency.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARREN
FROM PAUL ROSEN**

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

Senator Elizabeth Warren

Question 1

The Biden-Harris administration published an executive order nearly a year ago requiring notification of U.S. firms’ investments in China in sectors of national security concern. The EO also imposed prohibitions on certain U.S. investments in China. The Administration published preliminary rules for public comment in June, and senior officials have noted that the final rules will be published by the end of the year. I appreciate the administration’s efforts and understand formulating rules takes time. However, China’s efforts to indigenize microelectronics, quantum, and AI supply chains is rapidly accelerating, and I urge you to move as quickly as possible to finalize rules and fully implement these guardrails. Can you provide an update on the timing of the publication of the final rules and the implementation process?

Answer: On June 21, 2024, the Treasury Department issued a Notice of Proposed Rulemaking (NPRM) with draft regulations and explanatory discussion regarding the intent of—and to solicit comment on—the proposed rule. The period to submit written comments on the NPRM concluded on August 4, 2024, and comments were submitted by a wide range of stakeholders. The Treasury Department and our interagency colleagues are working expeditiously and taking the time needed to consider the public comments submitted on the proposed rule, make revisions as appropriate, and publish the final rule as soon as possible.

Question 2

The Outbound Investment Transparency Act (S. 2678) proposes an outbound investment screening regime similar to the Administration’s executive order published last year. Legislation would codify efforts that are currently being undertaken by emergency executive authority under IEEPA. How would codification of outbound investment screening via legislation ensure resiliency in the effort to protect critical U.S. technology supply chains?

Answer: The Treasury Department appreciates the interest and work of Congress in regulating outbound investment. Legislation that codifies the approach and authorities in E.O. 14105 with certain enhancements, such as direct hiring authority and statutory protections for the confidentiality of information, would benefit the effort being undertaken to address the advancement by countries of concern in sensitive technologies and products critical for the military, intelligence, surveillance, or cyber-enabled capabilities of such countries that could undermine U.S. national security, including the resilience and security of critical U.S. supply chains.

**RESPONSES TO WRITTEN QUESTIONS OF
SENATOR FETTERMAN FROM PAUL ROSEN**

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

Senator John Fetterman

Question 1

The Biden-Harris administration published an executive order about a year ago requiring notification of U.S. firms’ investments in China in sectors of national security concern. The EO also imposed prohibitions on certain U.S. investments in China. The Administration published preliminary rules for public comment in June, and senior officials have noted that the final rules will be published by the end of this year. We understand formulating rules takes time. However, China’s efforts to localize their microelectronics, quantum, and AI supply chains is rapidly accelerating.

Can you commit to publishing the final rules and beginning full implementation of the outbound executive order in the next three months?

Answer: On June 21, 2024, the Treasury Department issued a Notice of Proposed Rulemaking (NPRM) with draft regulations and explanatory discussion regarding the intent of—and to solicit comment on—the proposed rule. The period to submit written comments on the NPRM concluded on August 4, 2024, and comments were submitted by a wide range of stakeholders. The Treasury Department and our interagency colleagues are working expeditiously to consider the public comments submitted on the proposed rule, make revisions as appropriate, and publish the final rule as soon as possible.

Question 2

The Outbound Investment Transparency Act (S. 2678) introduced by Senators Casey and Comyn proposes an outbound investment screening regime similar to the Administration’s executive order published last year. Legislation would codify efforts that are currently being undertaken by emergency executive authority under IEEPA. OITA is currently under consideration for passage as part of this year’s NDAA.

How would codifying outbound investment screening via legislation further bolster the Biden-Harris Administration’s efforts to protect critical U.S. technology supply chains?

Answer: The Treasury Department appreciates the interest and work of Congress on regulating outbound investment. Legislation that codifies the approach and authorities in E.O. 14105 with certain enhancements, such as direct hiring authority and statutory protections for the confidentiality of information, would benefit the effort being undertaken to address the advancement by countries of concern in sensitive technologies and products critical for the military, intelligence, surveillance, or cyber-enabled capabilities of such countries that could undermine U.S. national security, including the resilience and security of critical U.S. supply chains.

Question 3

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

What are the drawbacks to relying on the president’s emergency powers to carry out an outbound investment screening program?

Answer: The President has authority pursuant to the National Emergencies Act and IEEPA to address the unusual and extraordinary threats to national security, such as that posed by the exploitation of certain U.S. outbound investments that would advance countries of concern in developing sensitive technologies and products that are critical to the military, intelligence, surveillance, or cyber-enabled capabilities of such countries. However, codification of authority with certain enhancements such as direct hiring authority and protection of confidential information under statute would benefit the program.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR SCOTT
FROM GRANT HARRIS**

**Questions for The Honorable Grant Harris, Assistant Secretary for Industry and Analysis,
Department of Commerce, from Ranking Member Tim Scott:**

- 1. In order to compete globally, the International Trade Administration must ensure that it has officers that can effectively compete with counterparts from other nations. Could you please detail the steps that your agency is taking to ensure that officers located in foreign countries have the language skills necessary to serve the region in which they are stationed?**

The International Trade Administration's Global Markets (GM) business unit oversees the U.S. and Foreign Commercial Service and manages foreign language training for the approximately 240 Foreign Service Officers employed in the Foreign Commercial Service (FCS). Under Global Markets, the Office of Global Talent Management directly manages all training in its Training & Development branch. A mandatory foreign language training program arranges all language training for Officers assigned to language-designated positions at foreign posts. In a given fiscal year, anywhere from fifteen to thirty officers begin training in as many as fifteen different languages at area language schools with proven track records of success.

The Inter-Agency Language Roundtable (ILR) scale is the way in which the U.S. Government measures and refers to language ability with 6 base levels from 0 (No Practical Proficiency) through 5 (Native or Bilingual Proficiency). As of September 2024, GM currently has 169 FCS Officers with active rated language proficiencies, including 142 FCS Officers with active scores of 3S/3R or above (Professional Working Proficiency in Speaking and Reading) across 19 languages. In addition, there is an identified tier of "super-hard" languages known as Category IV (including Chinese, Japanese, and Korean) to which GM trains to a lower standard of 2S/1R, consistent with Department of State Foreign Service Institute standards. GM has 42 FCS Officers scored at 2S/1R or above in these languages, with 27 Officers at 2S/1R and 15 Officers at the 3S/3R or higher.

- 2. Please provide a rough estimate of the number of individuals and the amount of time from employees of the Commerce Department that went into the development of President Biden's Executive Order on Outbound Investments and the related Notice of Proposed Rulemaking.**

A team of individuals from ITA's Industry and Analysis (I&A) unit worked on tasks related to the Outbound Investment Security Program. This core team also drew upon industry expertise across the I&A business unit involving each of the covered technology sectors and regularly received additional support from across the Department. This support included legal analysis from the Department's Office of the General Counsel, and support from the Bureau of Industry and Security and the National Institute of Standards and Technology. Across ITA, decision-makers and staff also worked together with Treasury and interagency colleagues on Treasury's proposed implementing regulations and conducted industry outreach sessions, including meetings with over 400 outside stakeholders to obtain feedback on the Advanced Notice of Proposed Rulemaking and the Notice of Proposed Rulemaking.

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

3. I am interested in better understanding the role your Department and your office played in implementing President Biden’s Executive Order on Artificial Intelligence.
- a. What is your overall takeaway from your Defense Production Act survey of the artificial intelligence industry?
 - b. How many private sector companies did the Commerce Department contact to implement the Defense Production Act provisions for the President’s Artificial Intelligence Executive Order?
 - c. What data or information did the Commerce Department request from private companies through the Defense Production Act?
 - d. Could you please explain how business confidentiality in the Defense Production Act limits your ability to share collected Defense Production Act survey information with Congress? Please be specific.
 - e. Do you plan to use any authorities under the Defense Production Act or International Emergency Economic Powers Act in relation to artificial intelligence?

The authority to collect information under the Defense Production Act has been delegated within the Department to the Bureau of Industry and Security (BIS). Accordingly, ITA would defer to BIS on the specific questions posed.

Regarding ITA’s role implementing the President’s Executive Order on Artificial Intelligence (AI), a key goal is the harmonization of international policies on AI in a way that facilitates trade and investment, while also ensuring responsible innovation and development. In addition, ITA has seen an uptick in requests from foreign counterparts for information and exchange of best practices on AI and digital issues, and ITA has ramped up its activity to meet this growing demand for engagement.

Our team within the I&A business unit within ITA is also actively engaged on the development and execution of U.S. digital policies, including in areas like data flows, privacy, and cybersecurity, that are critical to the responsible development of AI. I&A is working with foreign partners, industry, and the interagency to promote policies on these issues aligned with safeguarding national security, protecting consumers, and promoting U.S. competitiveness for businesses of all sizes.

As part of its work on AI, ITA is also engaging with foreign counterparts to share best practices and align regulatory approaches in various aspects of AI – including transparency, interoperability, and risk management. For example, the Department has

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

included AI in many Commerce-led government-to-government dialogues and worked to identify ways for industry experts, other Commerce bureaus, and the larger U.S. government to participate in policy workshops, public-private roundtables, and technical collaboration with foreign governments. ITA has engaged with U.S. startups and small and medium-sized enterprises (SMEs) to inform this work, as these types of businesses often have distinct needs and challenges in both adopting emerging technology like AI and navigating shifting regulatory and market access requirements. As this work continues, ITA has coordinated extensively within Commerce and across the U.S. Government to incorporate AI expertise in standards, intellectual property, security, policy, and other areas.

4. Mr. Harris, you oversee Defense Production Act surveys at the Commerce Department. Could you provide me with a list of non-defense industrial base areas where you see our industrial base falling short? Please be specific.

As mentioned in the previous response, the authority to collect information under the Defense Production Act has been delegated within the Department to BIS.

ITA’s Industry and Analysis (I&A) unit does provide data-driven analysis on globally connected supply chains and, last year, I&A launched the Supply Chain Center (Center) that serves as the main hub for that activity, drawing across the rest of the sector-specific subject matter experts within I&A and Commerce at large. The Center is facilitating collaboration across I&A, Commerce, and beyond in order to be proactive in getting ahead of supply chain challenges, strategic in setting priorities for policy focus and action based on data-driven risk analysis, a force multiplier in improving the targeting and effectiveness of U.S. Government investments, and a partner with industry in building resilient supply chains and supporting U.S. businesses in leading the industries of the future.

At this stage, I&A is analyzing the risk to supply chains from dependence on adversarial countries, which can cause the creation of chokepoints under that adversary’s control. In addition to geopolitical risks, I&A is also analyzing supply chains that may be vulnerable to shocks like natural disasters and global pandemics, such as the COVID-19 pandemic. I&A would welcome continued engagement with Congress as the Center’s analyses uncover vulnerabilities in critical supply chains and generate actionable policy options, as I&A first did with the semiconductor supply chain nearly a decade ago.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARREN
FROM GRANT HARRIS**

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

Questions for The Honorable Grant Harris, Assistant Secretary for Industry and Analysis,
Department of Commerce, from Senator Elizabeth Warren:

The Outbound Investment Transparency Act (S. 2678) proposes an outbound investment screening regime similar to the Administration’s executive order published last year. Legislation would codify efforts that are currently being undertaken by emergency executive authority under IEIPA.

1. **How would codification of outbound investment screening via legislation ensure resiliency in the effort to protect critical U.S. technology supply chains?**

The Outbound Investment Security Program addresses a critical gap in the U.S. Government’s technology protection toolkit that is necessary to address national security risks. The current Outbound Investment Security Program relies on the authorities provided to the President under the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and section 301 of title 3, United States Code, which are general in nature and are not specifically tailored to the Outbound Investment Security Program. The NEA requires annual action by the President to continue the declared national emergency declaration underlying the Outbound Investment Security Program (50 U.S.C. 1622(d)). Codification would ensure that the Outbound Investment Security Program continues without regard to such action. Legislation also could provide certain enhancements, such as statutory protections for the confidentiality of information and the ability to hire staff more quickly.

**RESPONSES TO WRITTEN QUESTIONS OF
SENATOR FETTERMAN FROM GRANT HARRIS**

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

Questions for The Honorable Grant Harris, Assistant Secretary for Industry and Analysis,
Department of Commerce, from Senator John Fetterman:

1. **Can you discuss why outbound investment screening is critical to U.S. national security? Why should we restrict U.S. investment in China? Why is it a good idea to better understand what U.S. investments are going to China?**

President Biden declared a national emergency in Executive Order (E.O.) 14105 which found that advancement by countries of concern in sensitive technologies and products critical for the military, intelligence, surveillance, or cyber-enabled capabilities of such countries constitutes an unusual and extraordinary threat to the national security of the United States. In particular, the People’s Republic of China (PRC) has exploited U.S. outbound investments, to help it develop its military capabilities. E.O. 14105 tasked the Secretary of the Treasury, in consultation with the Secretary of Commerce and, as appropriate, the heads of other relevant departments and agencies, with issuing regulations to establish the Outbound Investment Security Program, including both prohibited transactions and notifiable transactions. The E.O. also tasked Treasury with consulting with Commerce on key aspects of program development and administration, including on industry engagement and analysis of notified transactions. The notification requirement for certain U.S. person investments, as outlined in the most recent Notice of Proposed Rulemaking (NPRM) published on July 5, 2024 (89 FR 55846), would increase the U.S. Government’s visibility into transactions involving identified technologies and products relevant to the national security threat and would inform future policy development. Notifications of transactions would further provide the U.S. Government with a greater understanding of how U.S. capital and business expertise is supporting the development of certain technologies in the PRC, including semiconductors and microelectronics and artificial intelligence systems. Certain investments into those technologies as well as quantum information systems in the PRC would be subject to prohibition. Commerce will leverage its expertise to analyze information received from transaction notifications to inform the development of the Outbound Investment Security Program.

2. **What is your sense of how U.S. industry views outbound investment screening and the need to impose limited restrictions for national security reasons? How is the executive order and legislation driving firms behavior?**

The Department has conducted extensive engagement with various stakeholders across the U.S. business and investor community. Commerce, in consultation and coordination with the Treasury and State Departments, has developed and executed a robust strategy for industry engagement at each stage of the rulemaking process, including in the context of the issuance of the Advanced Notice of Proposed Rulemaking (ANPRM) and the Notice of Proposed Rulemaking (NPRM). Commerce has engaged in outreach with over 400 stakeholders in the last year, almost always with the Department of the Treasury.

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

During these engagements, Commerce received a wide range of questions, from questions on how narrowly scoped the Outbound Investment Security Program will be to questions about liability and enforcement provisions as well as inquiries about U.S. coordination with allies and partners. Many U.S. industry stakeholders encouraged close coordination with allies and partners and, where possible, joint approaches to outbound investment issues. Many stakeholders expressed gratitude that the Administration has been so forthcoming about the details of the program and its efforts to craft the program narrowly with an emphasis on bright-line rules. Many stakeholders also expressed their interest in understanding the details of the Outbound Investment Security Program’s proposed rules now to ensure strong future compliance.

The Outbound Investment Transparency Act (S. 2678) introduced by Senators Casey and Cornyn proposes an outbound investment screening regime similar to the Administration’s executive order published last year. Legislation would codify efforts that are currently being undertaken by emergency executive authority under IEEPA. OITA is currently under consideration for passage as part of this year’s NDAA.

3. How would codifying outbound investment screening via legislation further bolster the Biden-Harris Administration’s efforts to protect critical U.S. technology supply chains?

The Outbound Investment Security Program addresses a critical gap in the U.S. Government’s technology protection toolkit that is necessary to address national security risks. The current Outbound Investment Security Program relies on the authorities provided to the President under the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and section 301 of title 3, United States Code, which are general in nature and are not specifically tailored to the Outbound Investment Security Program. The NEA requires annual action by the President to continue the declared national emergency status underlying the Outbound Investment Security Program (50 U.S.C. 1622(d)). Codification would ensure that the Outbound Investment Security Program continues without the need for such action. The Administration supports efforts to codify the Outbound Investment Security Program as outlined in E.O. 14105 in a way that is consistent with the current parameters of the program. Legislation also could provide certain enhancements, such as statutory protections for the confidentiality of information and the ability to hire staff more quickly. The Commerce Department and its interagency partners are available to provide technical assistance with the drafting of legislation to ensure it is consistent with the current Outbound Investment Security Program.

4. What are the drawbacks to relying on the president’s emergency powers to carry out an outbound investment screening program?

Committee on Banking, Housing, and Urban Affairs
“Advancing National Security through Export Controls, Investment Security, and the
Defense Production Act”
July 25, 2024

The current Outbound Investment Security Program relies on the authorities provided to the President under the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and section 301 of title 3, United States Code, which are general in nature and are not specifically tailored to the Outbound Investment Security Program. The NEA requires annual action by the President to continue the declared national emergency status underlying the Outbound Investment Security Program. (50 U.S.C. 1622(d)). Codification would ensure that the Outbound Investment Security Program continues without the need for such action. The President’s emergency powers could be enhanced by statutory provisions for protecting the confidentiality of information and the ability to hire staff more quickly via direct hiring authority and resourcing.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR SCOTT
FROM LAURA TAYLOR-KALE**

Q.1. Dr. Taylor-Kale, in your opinion, what are the most pressing areas in our defense industrial base that must be addressed? Please be extensive and specific.

Could you provide a rough estimate of the cost to ensure resiliency for each of your listed areas?

A.1. Response not received in time for publication.


Q.2. In the FY24 NDAA, Congress provided you with the authority to access industrial base improvement projects with Australia and the U.K. in the case that a U.S. alternative did not exist. Could you provide me with an update on your utilization of that authority?

A.2. Response not received in time for publication.

Q.3. Under the Biden administration, we have seen DPA funds used at the Energy Department for Electric Heat Pumps to fight Climate Change and more broadly for biomanufacturing capabilities. With global challenges and the current shortcomings in our defense industrial base, how can we get this program back on track, with a focus on core defense capabilities, to ensure that we have a robust and resilient defense industrial base?

A.3. Response not received in time for publication.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

| | | | |
|--|--|-----------------------------------|--|
| DSP-05 050786865 | | Page 1 of 1 | |
|  | DENY | | |
| | License Number: 050786865 | Date Issued: 05/28/2024 | |
| | In accordance with the provisions of Title 22, Code of Federal Regulations, Section 126.7(a), the attached application is DENIED for the reasons indicated below. The United States Government position on this case consists of this 1 page decision memo and the attached 6 page application. Both must be present for the USG position to be valid. The POC for this USG action is Samantha Sison, 771-205-6768, sisonsm@state.gov. | | |
| REASONS: <u>Foreign Policy</u> (U) 1. Pursuant to 22 CFR 120.18(a)(1), and (2) of the ITAR, the Department of State may deny a license or other approval when the Department deems such action to be in furtherance of world peace, the national security or the foreign policy of the U.S., or is otherwise inadvisable; or believes that any party has violated 22 U.S.C. 2778 or the ITAR, or the terms of any U.S. Government export authorization. | | | |
| DSP-05 050786865 | | Page 1 of 1 | |

| U.S. Department of State Application for Permanent Export of Unclassified Defense Articles, Related Technical Data, and Defense Services | |
|--|--|
| OMB APPROVAL NO. 1495-0003 EXPIRATION DATE: 9/18/2025 ESTIMATED BURDEN: 1 HOUR | |
| *PAPERWORK REDUCTION ACT STATEMENT: Public reporting burden for this collection of information is estimated to average 1 hour per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (A/GIS/DIR) Washington, D.C. 20520. | |
| 1. Date Prepared 02/21/2024 | 2. DDTC Registration Code M24361 |
| 3. Country of Ultimate Destination Ecuador | 4. Probable Port of Exit from U.S. Port 1: Florida Port 2: Pennsylvania |
| 5. Applicant Applicant Is: Exporter Name: M. G. SUBER & ASSOCIATES, LLC Attention: Adeline Badillo Address: 213 Dawson Road City: Columbia State: South Carolina ZIP Code: 29223 Country: United States Telephone: 8037645797 | |
| 6. U.S. Government Personnel (not PM/DDTC) Familiar with Commodity No value selected. (Optional block) | |
| 7. Applicant Contact for Additional Information Name: Adeline Badillo Telephone: 8037645797 Extension: Name: Robert Suber Telephone: 8037645797 Extension: | |
| 8. Description of Transaction A. This application represents ONLY a completely new shipment B. This Application has related license # <input type="checkbox"/> was licensed to the country in Block 3 of the first page under license # <input type="checkbox"/> was licensed to other countries under license # <input type="checkbox"/> was returned without action under voided license # <input type="checkbox"/> was denied to the country in Block 3 of the first page under voided license # C. This Application is in reference to agreement # | |

D. If the commodity is being financed under

Not Applicable

Foreign Military Sale #
Case Numbers:

Foreign Military Financing #
Case Numbers:

Grant Aid Program #
Case Numbers:

E. This application is related to a disclosure filed with Defense Trade Controls Compliance

Yes No

9 - 13. Commodity Information

| Item | 9. Quantity | 10. Commodity | 11. USML Category | 12. \$ Value |
|-----------------|------------------------|---|-------------------|--------------|
| 1 | Quantity: 88 | 30 Round Rifle Magazine Defense Article Type: Hardware | I (x) | \$1,408 |
| 2 | Quantity: 2 | 60 Round drum magazine Defense Article Type: Hardware | I (h(1)) | \$263 |
| 13. Total Value | | | | \$1,671 |

14. Foreign End-User

Name: Policia Nacional del Ecuador - Grupo de Operaciones Especiales GOE de la Zona 6
 Address: Tadeo Torres 2-67 y Jose Alvear
 City: Cuenca, Provincia del Azuay, 170401
 Country: Ecuador

15. Manufacturer of Commodity

Name: Magpul
 Address: 8226 BEE CAVE RD
 City: Austin
 Country: United States
 State: Texas
 Zip Code: 78746

16. Foreign Consignee

Name: Policia Nacional del Ecuador - Grupo de Operaciones Especiales GOE de la Zona 6

| | |
|---|---|
| Address: | Tadeo Torres 2-67 y Jose Alvear |
| City: | Cuenca, Provincia del Azuay, 170401 |
| Country: | Ecuador |
| 17. Source of Commodity | |
| Name: | Magpul |
| Address: | 8226 BEE CAVE RD |
| City: | Austin |
| Country: | United States |
| State: | Texas |
| Zip Code: | 78746 |
| 18. Foreign Intermediate Consignee | |
| Name: | SECOHI-TRUCMONTCORP |
| Address: | Av. Maldonado S/N y Pujili esq. Quito - Ecuador |
| City: | Quito |
| Country: | Ecuador |
| Role: | In-country customs clearance agent |
| 19. U.S. Seller | |
| Name: | M. G. SUBER & ASSOCIATES, LLC |
| Address: | 213 Dawson Road |
| City: | Columbia |
| State: | South Carolina |
| ZIP Code: | 29223 |
| 20. Specific Purpose | |
| <input type="checkbox"/> Off-Shore procurement <input type="checkbox"/> Brokering (22 CFR 129) <input checked="" type="checkbox"/> Other | |
| <p>These articles will be used by the Azuay Zonal Headquarters of Special Ops of the National Police of Ecuador in risk operations in accordance with the institutional mission established in Article 163 that indicates that the National Police is a state institution of a civil, armed, technical, hierarchical, disciplined, professional and highly specialized, whose mission is to address citizen security and public order and protect the free exercise of rights and the security of people within the national territory.</p> | |
| 21. U.S. Consignor/Freight Forwarder | |
| Name: | Sovana Global Logistics |
| Address: | 45969 Nokes Blvd #175 |
| City: | Sterling |
| State: | Virginia |
| Zip Code: | 20166 |
| Name: | D.T. Gruelle Company Group LLC |
| Address: | 301 Moon Clinton Road |
| City: | Moon Township |
| State: | Pennsylvania |
| Zip Code: | 15108 |
| Name: | Air-Sea Forwarders, Inc. |

| | |
|-----------|------------------------------------|
| Address: | 10925 N.W. 27th Street Unit # 201 |
| City: | Miami |
| State: | Florida |
| Zip Code: | 33172 |
| Name: | ACD Cargo C/O Millennium Logistics |
| Address: | 10925 N.W. 27th Street |
| City: | Doral |
| State: | Florida |
| Zip Code: | 33172 |

22. Applicant's Statement

I, Adeline Badillo, an empowered official (22 CFR 120.67) or an official of a foreign government entity in the U.S., hereby apply for a license to complete the transaction described above; warrant the truth of all statements made herein; and acknowledge, understand and will comply with the provisions of 22 CFR 120-130, and any conditions and limitations imposed.

I am authorized by the applicant to certify the following in compliance with 22 CFR 126.13:

1. Neither the applicant, its chief executive officer, president, vice presidents, other senior officers or officials (e.g., comptroller, treasurer, general counsel) nor any member of its board of directors is:
 - a. the subject of an indictment for or has been convicted of violating any of the U.S. criminal statutes enumerated in 22 CFR 120.6 since the effective date of the Arms Export Control Act, Public Law 94-329, 90 Stat. 729 (June 30, 1976); or
 - b. ineligible to contract with, or to receive a license or other approval to import defense articles or defense services from, or to receive an export license or other approval from any agency of the U.S. Government;
2. To the best of the applicant's knowledge, no party to the export as defined in 22 CFR 120.68(a) has been convicted of violating any of the U.S. criminal statutes enumerated in 22 CFR 120.6 since the effective date of the Arms Export Control Act, Public Law 94-329, 90 Stat. 729 (June 30, 1976); or is ineligible to contract with, or to receive a license or other approval to import defense articles or defense services from, or to receive an export license or other approval from any agency of the U.S. Government; and

22 CFR 126.13 Certification

- a. I am authorized by the applicant to certify that the applicant and all the parties to the transaction can meet in full the conditions of 22 CFR 126.13 as listed above.
- b. I am authorized by the applicant to certify to 22 CFR 126.13. The applicant or one of the parties of the transaction cannot meet one or more of the conditions of 22 CFR 126.13 as listed above. A request for an exception to policy, as described in 22 CFR 127.11 of the ITAR, is attached.
- c. I am authorized by the applicant to certify to 22 CFR 126.13. The applicant or one of the parties of the transaction cannot meet one or more of the conditions of 22 CFR 126.13 as listed above. However that party has met the conditions imposed by the Directorate of Defense Trade Controls in order to resume standard submission of applications, not requiring an exception to policy as described in 22 CFR 127.11 of the ITAR.
- d. I am not authorized by the applicant to certify the conditions of 22 CFR 126.13. The applicant and all the parties to the transaction can meet in full the conditions of 22 CFR 126.13 as listed above. Please see the attached letter from an official that is authorized by the applicant to certify to the conditions of 22 CFR 126.13.
- e. I am not authorized by the applicant to certify the conditions of 22 CFR 126.13. The applicant or one of the parties of the transaction cannot meet one or more of the conditions of 22 CFR 126.13 as listed above. A request for an exception to policy, as described in 22 CFR 127.11 of the ITAR, and a letter from an official that is authorized by the applicant to certify to the conditions of 22 CFR 126.13 are attached.
- f. I am not authorized by the applicant to certify to 22 CFR 126.13. The applicant or one of the parties of the transaction cannot meet one or more of the conditions of 22 CFR 126.13 as listed above. However that party has met the conditions imposed by the Directorate of Defense Trade Controls in order to resume standard

submission of applications, not requiring an exception to policy as described in 22 CFR 127.11 of the ITAR. Please see the attached letter from an official that is authorized by the applicant to certify to the conditions of 22 CFR 126.13.

Compliance with 22 CFR 130

- This transaction does not meet the requirements of 22 CFR 130.2.
- This transaction meets the requirements of 22 CFR 130.2. The applicant or its vendors have not paid, nor offered, nor agreed to pay, in respect of any sale for which a license or approval is requested, political contributions, fees or commissions in amounts as specified in 22 CFR 130.9(a).
- The applicant or its vendors have paid, or offered, or agreed to pay, in respect of any sale for which a license or approval is requested, political contributions, fees or commissions in amounts as specified in 22 CFR 130.9(a). Information required under 22 CFR 130.10 is attached.
- I am not authorized by the applicant to certify the conditions of 22 CFR 130.9(a). Please see the attached letter for such certification.

CONDITIONS OF ISSUANCE

1. This license is issued under the conditions cited in 22 CFR 120-130, including the conditions and limitations as applicable, that:
 - A. It shall not be construed as implying U.S. Government approval or commitment to authorize future exports of any defense article (hardware or technical data) on the U.S. Munitions List (USML), or a U.S. Government commitment with regard to any proposed manufacturing license, technical assistance or distribution agreement that may result from a license or other approval.
 - B. If a license is issued for technical data only, it does not authorize the export of any hardware; if a license is issued for hardware only, it does not authorize the export of any technical data, unless specifically authorized by an exemption.
 - C. The issuance of this license does not release the applicant, or anyone acting on their behalf, from complying with other requirements of U.S. law and regulations.
 - D. This transaction may be subject to end-use monitoring by the United States Government.
2. The prior written approval of the Department of State, Directorate of Defense Trade Controls, must be obtained before USML defense articles exported from the U.S. using a license or other approval, to include an ITAR exemption, may be resold, transferred, diverted, transshipped, re-exported to, or used in any country, or by any end user or for any end use, other than that described on the license or other approval.

DISPOSITION OF LICENSE

The final disposition of this license shall be in accordance with 22 CFR 123.22(c).

ENDORSEMENT

Indicate below which COMMODITY is BEING EXPORTED and maintain a CONTINUING BALANCE of the remaining value:

| SHIPMENT DATE | QUANTITY | COMMODITY | SHIPMENT VALUE | XTN/ITN | INITIALS | PORT OF EXIT/ ENTRY |
|-------------------------|----------|-----------|----------------|---------|----------|---------------------|
| TOTAL AUTHORIZED VALUE: | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| REMAINING BALANCE: | | | | | | |

| SHIPMENT DATE | QUANTITY | COMMODITY | SHIPMENT VALUE | XTN/ITN | INITIALS | PORT OF EXIT/ ENTRY |
|--|----------|-----------|----------------|---------|----------|---------------------|
| NOTE: Continuation of additional shipments must be authenticated by use of continuation sheets in the U.S. Customs handbook. | | | | | | |



M.G. Suber & Associates, LLC
213 Dawson Road Columbia, SC
29223 USA

July 17th, 2024

Dear Senator Scott and Banking Committee,

M.G. Suber & Associates, LLC, a small minority-owned business in the heart of South Carolina, specifically Columbia, has been thriving for an impressive 38 years. Specializing in exporting defense, security and sporting articles to various countries, the company prides itself on its high compliance standards, earning a well-known and respected reputation in the industry. We were chosen as Exporter of the Year for South Carolina by the Small Business Administration in 2022.

On July 1st, 2024, \$71.1 million dollars' worth of our export licenses (see attached list) were revoked by the U.S. Department of Commerce's Bureau of Industry and Security. The plan, as proposed under the IFR, aims to put hardworking American companies out of business in furtherance of human rights convictions.

We ensure export compliance by abiding by regulations from various agencies such as the Department of Commerce, Department of State, ATF, and OFAC. Our thorough processes, programs, and procedures include conducting in-depth background checks on all our customers. It is our priority to adhere to these rules and ensure that our end users do the same.

Free commerce has been infringed upon with the stroke of a pen from the administration. We have lost the ability to sell to customers in countries with stricter policies than those in the US on how they sell their products. As a country that stands for the 2nd amendment, to prohibit our allied countries from exercising what we believe to be an innate fundamental right is a violation of human rights on its own.

The rule's impact on our foreign sales has led to our default on multiple contracts with our customers, straining the US's relationships with our allies. The \$70 plus million losses will significantly affect the American economy, surpassing the size of a small South Carolina office. Unfortunately, removing these jobs will not only cost us economically but also in terms of livelihoods, and family stability within the manufacturing, sales, and logistics sectors.

Our company stands strong in supporting our military, state, and local families. We proudly supply to the US government under small business set asides and extend our reach to allied countries' government end users and reputable foreign distributors. Despite our commitment to export compliance excellence while attending every export compliance conference, keeping the regulations on hand and interfacing with the export control agencies as much as possible to ensure such excellence in compliance, our existence is threatened by a ruling from this administration. Urgent action is needed to ensure our continued contribution to the community and the economy.



M.G. Suber & Associates, LLC
213 Dawson Road Columbia, SC
29223 USA

There is no question that these changes were put into effect to reverse policies implemented in the previous Trump administration.

Respectfully,

A handwritten signature in blue ink, appearing to read 'R. Suber', is written over a light blue rectangular background.

Robert G. Suber

Chief Executive Officer & Owner

| Revoked license Number | Country | Commodity | Quantity | Total Price |
|------------------------|--------------------|---|----------|-----------------|
| D1334113 | Dominican Republic | Shotguns | 105 | \$21,105.00 |
| D1226442 | Trinidad & Tobago | Pistols / Shotguns | 1500 | \$1,700,000.00 |
| D1289673 | Panama | Ammunition | 1000 | \$3,000.00 |
| D1215177 | El Salvador | Pistols/Rifles/Magazines | 1500 | \$492,710.00 |
| D1204997 | Panama | Pistol and Rifle Magazines | 12000 | \$129,520.00 |
| D1226140 | Guatemala | Revolvers & Pistols | 50 | \$74,592.00 |
| D1217695 | Trinidad & Tobago | Pistols / Shotguns | 900 | \$510,000.00 |
| D1244422 | Guatemala | Rifles/pistols/magazines | 2200 | \$76,000.00 |
| D1236886 | El Salvador | Pistol/rifles & revolvers | 130 | \$241,450.00 |
| D125438 | Trinidad & Tobago | Ammunition | 700000 | \$1,050,000.00 |
| D1212499 | Guatemala | Pistols/Rifles/Magazines | 65250 | \$24,416,720.00 |
| D1216327 | Guatemala | Shotguns/rifles/pistols/ magazines | 15200 | \$12,400,000.00 |
| D1229377 | Trinidad & Tobago | shotguns/rifles | 150 | \$125,000.00 |
| D1213602 | El Salvador | pistols/rifles & Shotguns & Magazines & revolvers | 1958 | \$911,076.00 |
| D1211784 | Guatemala | Magazines | 95 | \$3,230.00 |
| D1229677 | Panama | Pistols/Revolvers/Shotguns | 192 | \$119,884.00 |
| D1185177 | Bahamas | Shotguns | 380 | \$239,040.00 |
| D1228030 | Panama | Magazines/ Pistols | 1650 | \$27,850.00 |
| D1214989 | Panama | Revolvers/ Pistols/Shotguns/ Magazines | 400 | \$247,658.00 |
| D1235601 | Trinidad & Tobago | magazines | 1400 | \$35,650.00 |
| D1226174 | Panama | shotguns/pistols/rifles/ magazines | 1210 | \$715,230.00 |
| D1207399 | Guatemala | revolvers/pistols | 38 | \$38,287.00 |
| D1226902 | Bahamas | Rifles | 43 | \$38,012.00 |
| D1213579 | Guatemala | Magazines | 2000 | \$24,800.00 |
| D1222443 | Panama | Pistols/Rifles/Revolvers | 3000 | \$3,105,000.00 |
| D1214287 | Bahamas | Shotguns | 360 | \$239,040.00 |
| D1239594 | El Salvador | Pistols & Rifles | 450 | \$685,995.00 |
| D1234514 | Panama | Pistols & Rifle | 2000 | \$1,590,000.00 |
| D1285499 | Bahamas | Magazines | 500 | \$15,000.00 |
| D1274107 | Bahamas | Shotguns/rifles/pistols | 1020 | \$453,585.00 |
| D1265896 | Suriname | Shotguns | 100 | \$98,000.00 |
| D1267601 | Guatemala | Magazines/Spare parts | 1530 | \$38,400.00 |
| D1241888 | Brazil | Rifles & Pistols | 1000 | \$795,000.00 |
| D1242966 | Trinidad & Tobago | Conversion Kits/rounds | 5006 | \$1,540,350.00 |
| D1288613 | Panama | Shotguns/Pistols/Rifles/Revolvers/ Magazines | 7440 | \$1,800,000.00 |
| D1243342 | Panama | Shotguns/Pistols/Rifles/Revolvers/ Magazines | 1340 | \$759,153.00 |
| D1245674 | El Salvador | Pistols/Rifles & Revolvers & Shotguns | 150 | \$184,650.00 |
| D1243844 | Suriname | Shotguns and rifles | 65 | \$64,200.00 |
| D1241950 | Jamaica | Shotguns | 100 | \$88,400.00 |
| D1251586 | Guatemala | pistols/rifles & Shotguns & Magazines | 1300 | \$965,500.00 |
| D1196743 | Trinidad & Tobago | Pistol & Shotguns | 1500 | \$1,700,000.00 |
| D1196207 | Trinidad & Tobago | Pistols | 80 | \$145,560.00 |
| D1203540 | El Salvador | Magazines | 4000 | \$100,000.00 |
| D1194790 | Guatemala | Revolvers/Pistols | 228 | \$57,067.00 |
| D1282020 | El Salvador | Pistols & Shotguns & ammo | 445525 | \$2,123,925.00 |
| D1313751 | Pakistan | Ammunition | 41300 | \$18,999.00 |
| D1302490 | Dominican Republic | Shotguns | 20 | \$7,100.00 |
| D1202779 | Trinidad & Tobago | Shotguns | 150 | \$81,600.00 |
| D1202598 | Suriname | Shotguns/Pistols | 1999 | \$1,039,903.00 |
| D1193680 | El Salvador | Shotgun & Ammunition | 64000 | \$15,005.00 |
| D1204983 | Bahamas | Rifles | 93 | \$61,924.00 |
| D1305030 | Dominican Republic | Shotgun & Revolvers | 29 | \$16,804.00 |
| D1309345 | Dominican Republic | Revolver & Shotguns | 38 | \$20,590.00 |
| D1297384 | Bahamas | Pistols & Shotguns | 620 | \$480,000.00 |
| D1307963 | Suriname | Pistols | 50 | \$75,000.00 |
| D1296355 | Guatemala | Pistols & Rifles & Magazines | 450 | \$159,000.00 |
| D1296296 | Panama | Shotguns & Pistols & Rifles & Magazines | 7000 | \$5,323,000.00 |
| D1292794 | Bahamas | Pistols | 25 | \$20,000.00 |
| D1305353 | Belize | Pistols/Rifles/ Shotguns | 1350 | \$771,480.00 |
| D1318988 | Guatemala | Shotguns/Rifles | 1115 | \$1,115,000.00 |
| D1322563 | Suriname | Shotguns | 200 | \$120,000.00 |

| | | | | |
|----------|--------------------|----------------------|-----|-----------------|
| D1321723 | Panama | Pistols & Rifles | 250 | \$400,000.00 |
| D1334139 | Dominican Republic | shotguns | 75 | \$15,075.00 |
| D1334123 | Dominican Republic | Shotguns | 25 | \$5,025.00 |
| D1334097 | Dominican Republic | Shotguns | 25 | \$5,025.00 |
| D1336492 | Dominican Republic | Shotguns | 25 | \$9,200.00 |
| D1338488 | Dominican Republic | Shotguns & revolvers | 35 | \$21,105.00 |
| D1338487 | Dominican Republic | Shotguns & Revolvers | 90 | \$62,674.00 |
| D1334126 | Dominican Republic | Shotguns | 20 | \$4,020.00 |
| D1334074 | Dominican Republic | Shotguns | 100 | \$20,100.00 |
| D1241746 | Dominican Republic | Pistols and Rifles | 2 | \$3,000.00 |
| D1333986 | Dominican Republic | revolvers & shotguns | 250 | \$180,000.00 |
| D1304018 | Kazakhstan | ights/ Magrifier | 22 | \$11,842.00 |
| | | | | \$71,124,019.00 |