EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

January 15 2024 - Volume 19, Issue 23

BUREAU OF INDUSTRY AND SECURITY
December 4, 2024
www.bis.gov

IMPORTANT information for users of the Bureau of Industry and Security (BIS) web-based application software system SNAP-R:

Please verify that the email address in your user profile in SNAP-R is unique to you, correct, and valid.

Changes are coming soon: SNAP-R will be making enhancements to improve usability and security. As part of this enhancement, the current Login ID will be replaced with your unique email address in SNAP-R to enable the required two-factor authentication procedures. As such, each user will need to update their profile with a unique email address by January 31, 2025.
What do you need to do to maintain account access?

- Log into SNAP-R now and use the Manage User Profile function within your account to update your e-mail.
- Please also contact your company's/firm's SNAP-R Administrators to validate that your email is unique within your CIN account. (If you are the only user of your CIN account, this step is not necessary.)
- If you are an Administrator for your CIN account, please verify now that every user in your company/firm has a unique, active email address, and add or change email addresses as necessary using the SNAP-R Self-Management function.
- Please note: For users, firms, companies that may manage multiple CIN accounts, you can use the same email address across all your CIN accounts.

This message is currently posted on the SNAP-R homepage. The BIS Office of Exporter Services appreciates action by users of the SNAP-R software to take these steps now.

NEWSLETTER NOTES

FOR IMMEDIATE RELEASE
December 5, 2024
www.bis.gov

Commerce Issues Final Rule to Formalize ICTS Program

Final Rule Formalizes Implementation of ICTS Program Authorities to Address Undue and Unacceptable Foreign Adversary Risks to ICTS Transactions in the United States

WASHINGTON, D.C. – Today, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) issued a final rule cementing the procedures it will follow in investigating foreign adversary threats to information and communications technology and services (ICTS) transactions that may harm U.S. national security, pursuant to Executive Order (EO) 13873: Securing the Information and Communications Technology and Services Supply Chain.

This final rule demonstrates the Biden-Harris Administration's proactive efforts to address the potential national security risks associated with the ICTS supply chain and the abuse of U.S. critical infrastructure by foreign adversaries. It is a significant step in formalizing the operations of the Office of Information and Communications Technology and Services (OICTS), which was established within BIS in March 2022 to implement EO 13873 and related executive orders.

Since its formation, OICTS has completed or undertaken several key investigations and rulemakings. In June 2024, OICTS announced a first-of-its-kind final determination prohibiting Kaspersky Lab, Inc., the U.S. subsidiary of a Russia-based anti-virus software and cybersecurity company, from selling its software within the United States or providing updates to software already in use, amongst other activities.

Additionally, in September 2024, OICTS issued a proposed rule that would prohibit the sale or import of connected vehicles integrating specific pieces of hardware and software, or those components sold separately, with a sufficient nexus to the People's Republic of China (PRC) or Russia. These actions underscore the critical role of OICTS in protecting American technologies and services from potentially malicious foreign adversary intervention or interference.

"This final rule clarifies and strengthens BIS's existing authorities to investigate, mitigate, and prohibit ICTS transactions involving our foreign adversaries. It significantly enhances our ability to protect the resilience of our national infrastructure and technology and communications sectors," said Under Secretary of Commerce for Industry and Security Alan F. Estevez. "The further formalization of the OICTS is an important part of a pivotal year in the office's growth as it continues to advance U.S. national security."

"Today's rule affirms the Department's commitment to preventing foreign adversaries from using U.S. technology and communications systems to harm U.S. persons or critical infrastructure," said OICTS Executive Director Elizabeth Cannon. "The rule makes important updates to the processes our office uses to identify and mitigate risks and enforce our regulations on foreign adversary ICTS in the United States."

(*Continued On The Following Column)

An interim final rule published on January 19, 2021, solicited public comments on how the Department should implement various provisions of EO 13873. The final rule addresses feedback from the public on a number of issues, including the scope of the rule, the timeline for completing investigations, the procedures the Department will follow in making determinations, and the role of the Department's interagency partners.

Changes made in today's final rule include consolidating the list of technologies within the scope of the rule, outlining the sources of information the Secretary of Commerce may consider when formulating Initial and Final Determinations, and refining the recordkeeping requirements for parties to transaction(s). The Department intends these changes to be consistent with industry and public concerns regarding potential foreign adversary threats to the ICTS supply chain.

The text of the final rule released today is available on the Federal Register's website here.

For more information, visit https://www.bis.gov.

****

FOR IMMEDIATE RELEASE
Friday, December 6, 2024
Media Contact:
Office of Public Affairs, publicaffairs@doc.gov

Biden-Harris Administration Announce Preliminary Terms with Coherent, SkyWater, and X-Fab to Advance U.S. Supply Chain Security

Proposed CHIPS Investments in Minnesota and Texas Would Help Enhance Production Capacity of Important Semiconductor Manufacturing Components

Today, the Biden-Harris Administration announced that the U.S. Department of Commerce signed three separate preliminary memoranda of terms (PMT) under the CHIPS and Science Act to provide up to $33 million in proposed direct funding to Coherent, up to $16 million in proposed direct funding to SkyWater Technology Foundry Inc., and up to $50 million in proposed direct funding to X-Fab. President Biden signed the bipartisan CHIPS and Science Act to usher in a new era of semiconductor manufacturing in the United States, bringing with it a revitalized domestic supply chain, good-paying jobs, and investments in the industries of the future. The proposed investment in Coherent would support the expansion and modernization of the company's existing facility in Sherman, Texas and is expected support approximately 70 direct jobs. The proposed investment in SkyWater would support the modernization of its existing facility in Bloomington, Minnesota and is expected to create approximately 70 jobs. The proposed investment in X-Fab would support the modernization and expansion of its existing silicon carbide fab in Lubbock, Texas while and is expected to create up to an estimated 150 jobs.

"The Biden-Harris Administration's bipartisan CHIPS and Science Act is making targeted investments to meet market demands for technology critical to our national and economic security," said **U.S. Secretary of Commerce Gina Raimondo**. "Today's proposed investments across Texas and Minnesota would help bolster domestic chip production and help secure our supply chain for decades to come."

(*Continued On The Following Page)

"Today's three semiconductor announcements recognize that America's innovative edge is rooted in communities like Sherman and Lubbock, Texas and Bloomington, Minnesota. The President and Vice President's CHIPS & Science Act is creating jobs, supporting small businesses, and securing the resilience of our supply chains all throughout the United States," said **National Economic Advisor Lael Brainard.**

The proposed funding announced today would support the following projects:

- **Coherent (Sherman, Texas):** The Biden-Harris Administration's proposed investment of up to $33 million would support the modernization and expansion of a state-of-the-art manufacturing cleanroom in Coherent's existing 700,000 square-foot facility in Sherman, Texas to establish the world's first 150mm indium phosphide (InP) manufacturing line by adding advanced wafer fabrication equipment to produce InP devices at scale. InP optoelectronic devices are widely used in applications such as datacom and telecom transceivers, including for AI infrastructure applications, advanced sensing for consumer electronics, and medical and automotive applications. The increased production of Coherent's InP devices, which are increasingly growing in demand, would allow the U.S. to advance supply chain resiliency and technological leadership and create approximately 70 jobs.

- **SkyWater Technology (Bloomington, Minnesota):** The Biden-Harris Administration's proposed investment of up to $16 million in SkyWater would support the modernization of its existing facility in Bloomington, Minnesota to improve the quality of production and wafer services by replacing equipment, upgrading the facility's cleanroom and space and IT systems, and increase overall production capacity of 90nm and 130nm wafers by approximately 30%. SkyWater's Bloomington facility offers its customers in the aerospace and defense, automotive, biomedical and industrial markets the ability to prototype and scale to volume production differentiated technology. The company is a Department of Defense (DoD) Trusted **F**oundry; as a result of proposed CHIPS funding, the company would be able to improve productivity and enhance operational sustainability to support DoD missions as well as grow its commercial business. The proposed CHIPS investment would build upon the company's 40-year history in Bloomington, Minnesota and is expected to create approximately 70 jobs. SkyWater's community workforce development efforts include its ongoing partnership with Hennepin Technical College, Greater Minneapolis Saint Paul Regional Economic Development Partnership, and the University of Minnesota Twin Cities and working with the Minnesota CHIPS coalition to support its short and long-term workforce development goals. In addition, the State of Minnesota's Forward Fund would provide $19 million in dedicated funding to support this proposed project.

(*Continued On The Following Column)

- **X-Fab (Lubbock, Texas):** The Biden-Harris Administration's proposed investment of up to $50 million would support the expansion and modernization of X-Fab's Silicon Carbide (SiC) foundry facility, the only high-volume SiC foundry in the U.S. SiC technology is key to the global decarbonization efforts in the automotive and industrial sectors and offers multiple advantages over conventional silicon-based technologies for high-power applications. The proposed CHIPS funding would bolster supply resiliency for critical infrastructure markets that were adversely impacted by foundry capacity shortages and supply chain disruptions during the COVID-19 pandemic. The proposed terms provide support for workforce development efforts including X-Fab's current partnerships with Texas Tech College of Engineering, South Plains College, Western Technical College, Lubbock Area United Way, SEMI Foundation, and the Lubbock Economic Development Alliance. The proposed CHIPS investment would create an estimated 150 jobs.

"This proposed investment allows Coherent to accelerate its industry leadership in InP technology and manufacturing," said **Dr. Giovanni Barbarossa, Chief Strategy Officer and President, Materials Segment, for Coherent**. "We are very excited for this opportunity to accelerate the delivery of world-class optoelectronic products that will enable America's economic future."

"We are pleased to receive this important proposed CHIPS funding, including the Advanced Manufacturing Investment Tax Credit to expand our nation's onshore capacity. We've been the beneficiary of many government program awards over the past several years, and we're proud of our role in helping to expand the domestic microelectronics infrastructure and strengthen the U.S. supply chain," said **SkyWater CEO, Thomas Sonderman.** "As America's Trusted Foundry, through our business model and expanding capabilities, we are creating a national asset for technology development, which is in a critical state domestically. We have been working to meet the specific needs of the Defense Industrial Base and commercial companies developing the technologies of the future. The proposed investments today are another milestone along this path."

"The demand for silicon carbide technologies will be strong for the long term, and we are proud to provide solutions that support the transition to electric mobility and renewable energy sources, said**Rico Tillner, CEO of X-FAB Texas**. X-FAB Texas' silicon carbide technologies are leading in quality and yield and provide a long-term perspective for the site. The proposed CHIPS funding will support the future success of X-FAB Texas and will contribute to the establishment of a domestic supply chain for silicon carbide."

Coherent, SkyWater and X-Fab have indicated they plan to claim the Department of the Treasury's Advanced Manufacturing Investment Credit (CHIPS ITC), which is 25% of qualified capital expenditures. Click here to learn more about the tax credit.

(*Continued on the Following Page)

As explained in its first Notice of Funding Opportunity, the Department of Commerce may offer applicants a PMT on a non-binding basis after satisfactory completion of the merit review of a full application. The PMT outlines key terms for a potential CHIPS incentives award, including the amount and form of the award. The award amounts are subject to due diligence and negotiation of award documents and are conditional on the achievement of certain milestones. After a PMT is signed, the Department of Commerce begins a comprehensive due diligence process on the proposed projects and continues negotiating or refining certain terms with the applicant. The terms contained in any final award documents may differ from the terms of Coherent, SkyWater and X-Fab's PMT's being announced today.

About CHIPS for America
CHIPS for America has awarded over $19 billion of the over $36 billion in proposed incentives funding allocated to date. These announcements across 20 states are expected to create over 125,000 jobs. Since the beginning of the Biden-Harris Administration, semiconductor and electronics companies have announced over $450 billion in private investments, catalyzed in large part by public investment. CHIPS for America is part of President Biden and Vice President Harris's economic plan to invest in America, stimulate private sector investment, create good-paying jobs, make more in the United States, and revitalize communities left behind. CHIPS for America includes the CHIPS Program Office, responsible for manufacturing incentives, and the CHIPS Research and Development Office, responsible for R&D programs, that both sit within the National Institute of Standards and Technology (NIST) at the Department of Commerce. Visit chips.gov to learn more.
****

FOR IMMEDIATE RELEASE

December 6, 2024
www.bis.gov

BIS Publishes Assessment on the Use of Mature-Node Chips

WASHINGTON, D.C. – Today, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) is releasing a report on the use of mature-node semiconductor chips, or legacy chips, in supply chains that directly or indirectly support U.S. critical infrastructure. The report includes key findings related to U.S. companies' use of legacy chips manufactured by entities based in the People's Republic of China (PRC).
The report, based on data BIS collected pursuant to an authority under the Defense Production Act (DPA), shows:

- Companies that sell products containing legacy chips continue to lack visibility into their semiconductor supply chains. About half of surveyed companies were unable to determine whether their products contained any chips manufactured by PRC-based foundries.
- Based on the information respondents provided, U.S. companies' use of chips made in PRC-based foundries is pervasive. More than 2/3 of their products contain PRC-origin chips. However, these legacy chips represent a limited share of the total number of chips used in those products.
- Capacity expansion in China has already begun to cause pricing pressure that may weaken U.S. chip suppliers' competitive positions.

(*Continued on the Following Column)

"We are committed to creating a level playing field in the semiconductor industry to ensure that U.S. companies, and those in like-minded countries, can compete. But unfair practices from the PRC to expand legacy chip production will create significant challenges for U.S. economic and national security," said **Under Secretary of Commerce for Industry and Security Alan F. Estevez**. "Our survey results indicate that companies remain shockingly unaware of the sources of chips used in their products. While government cannot act alone, more action is needed to build strong, diverse, and resilient semiconductor supply chains."

"This work has provided invaluable data that will help the U.S. government continue building secure semiconductor supply chains," said **Assistant Secretary of Commerce for Export Administration Thea D. Rozman Kendler**. "Legacy chips are essential components in almost every part of our critical infrastructure, and it's imperative we understand our exposure to any supply chain risks and act accordingly to address them."

In January 2024, BIS initiated a DPA survey and assessment to learn how companies are sourcing these mature-node semiconductors. The survey and assessment were initiated at the direction of the Secretary of Commerce to bolster the Department's ongoing work to develop robust semiconductor supply chains, support domestic production of semiconductors, and protect U.S. national security.
The report's findings illuminate how U.S. companies are currently directly and indirectly sourcing legacy chips and the extent of the use of chips manufactured by companies based in the PRC in critical U.S. industries, to include telecommunications, automotives, medical devices, and the defense industrial base.

The report's findings will help inform future U.S. government actions to address PRC overconcentration and oversupply concerns, as well as companies' lack of visibility into the supply chains for these critical semiconductor components. The Department remains committed to securing critical supply chains for semiconductors and safeguarding the U.S. economy from the distorting effects of non-market activity.

Review the report here.
For more information, visit www.bis.gov.
****

The Syrian People Finally Have a Reason for Hope

12/08/2024 05:50 PM EST

Antony J. Blinken, Secretary of State

After 14 years of conflict, the Syrian people finally have reason for hope. The Assad regime's refusal since 2011 to engage in a credible political process and its reliance on the brutal support of Russia and Iran led inevitably to its own collapse. The United States strongly supports a peaceful transition of power to an accountable Syrian government through an inclusive Syrian-led process. During this transitional period, the Syrian people have every right to demand the preservation of state institutions, the resumption of key services, and the protection of vulnerable communities.

We will be closely monitoring developments as they unfold and engaging with our partners in the region. We will support international efforts to hold the Assad regime and its backers accountable for atrocities and abuses perpetrated against the Syrian people, including the use of chemical weapons and the unjust detention of civilians such as Austin Tice. We have taken note of statements made by rebel leaders in recent days, but as they take on greater responsibility, we will assess not just their words, but their actions. We again call on all actors to respect human rights, take all precautions to protect civilians, and to uphold international humanitarian law.

****

FOR IMMEDIATE RELEASE
December 9, 2024

www.bis.gov

BUREAU OF INDUSTRY AND SECURITY

Office of Congressional and Public Affairs

OCPA@bis.doc.gov

Assistant Secretary for Export Enforcement Matthew S. Axelrod Delivers Remarks at the Practicing Law Institute's Coping with U.S. Export Controls and Sanctions Conference

Washington, D.C. December 9, 2024

Remarks as Prepared for Delivery

Every morning, as I drive my car into the Commerce Department parking lot, I pass under a stone relief sculpted on the outside of the building. The relief, which depicts a life preserver on top of an anchor, bears the year 1838 and the inscription "Steamboat Inspection." Back in 1838, steamboat disasters were common. From boiler explosions to collisions, traveling by steamboat had significant safety risks. To help mitigate those risks, Congress created the Steamboat Inspection Service, tasking it with protecting the safety of steamship crews and passengers. The Inspection Service examined the hulls and machinery of steam vessels and administered laws requiring those vessels to carry life-saving equipment. In 1903, Congress transferred the Service to the Commerce Department, then called the Department of Commerce and Labor. And until the end of World War II, when its functions were eventually transferred to the U.S. Coast Guard, steamboat inspection work was among the Department's core functions.

(*Continued On The Following Column)

Seeing that stone relief each day reminds me just how drastically the Commerce Department's mission has changed since the early 1900s. Today, instead of steamboats powering the American economy, it's semiconductors. And instead of worrying about safety risks for individual steamboat crewmembers and passengers, we're focused on national security risks shared by every American. At the Bureau of Industry and Security (BIS), my team is responsible for preventing nation-state adversaries from obtaining sensitive U.S. technologies to modernize their militaries, enable human rights abuses, and advance their weapons-of-mass-destruction (WMD) programs. We work to keep our country's most sensitive technologies out of the world's most dangerous hands. That world looks a lot different today than it did when the Commerce Department was first created. And so does the Department's place in it, with BIS now playing a critical role in protecting our country's national security.

I started at Commerce in December 2021, just two months before Russia's full-scale invasion of Ukraine. And what I said to my team that first day rings just as true three years later: Export Enforcement, now more than ever before, is the tip of the spear when it comes to preventing sensitive U.S. technologies from being put to malign purposes by our adversaries.

Our enforcement authorities under the Export Control Reform Act are mighty. We have the power to investigate export violations and impose administrative and, with the support of the Department of Justice, criminal penalties. We also have the regulatory ability to impose broad controls on entities of national security or foreign policy concern.

But our budget – aptly described by Secretary Gina Raimondo as still less than "the cost of a few fighter jets" – has not kept pace with those authorities or with the heightened importance of our mission. There were more than 32 million exports of dual-use items in 2021, the year I came on board. And we have approximately 150 enforcement agents and 40 analysts to detect and investigate exports that violate our rules. You do the math. There's just no possible way we can protect U.S. technology through investigation alone.

That's why, on my very first day, I told everyone in Export Enforcement that we needed to be strategic and intentional about how we maximize our finite resources to best meet this critical national security moment. I told them that, during my tenure, we were going to focus on three "Ps" – prioritized enforcement, profile, and partnerships. By prioritizing our enforcement, enhancing our profile, and strengthening our partnerships, I said, we can ensure that we are putting the resources we do have to their highest and best use. Those three "Ps" were our focus areas for the last three years. So, let's take a look at how well we did executing on them.

Prioritized enforcement

I'll start with how we've prioritized our enforcement efforts. We don't have the resources to monitor every export or investigate every potential violation. That means every investigation we choose to do actually carries with it an implicit choice not to do others. Because our resources are limited, it's a zero-sum game. Accordingly, we've needed to be relentless in our thinking about how to use our finite resources to have the biggest national security impact.

(*Continued on the Following Page)

That's why, in February 2022, we launched the Disruptive Technology Strike Force with the Department of Justice to protect a prioritized group of advanced technologies – such as quantum computing, advanced semiconductors, and hypersonics – from illegal acquisition and use by nation-state adversaries like Russia, China, and Iran. The Strike Force brings together experienced prosecutors and agents from BIS, the Federal Bureau of Investigation (FBI), Homeland Security Investigations (HSI), and the Defense Criminal Investigative Service (DCIS) to form operational cells in seventeen different locations across the country. These agents and prosecutors are supported by an interagency analytical effort organized out of the agencies' headquarters here in Washington, D.C.

Since its inception, the Strike Force has publicly charged 25 criminal cases, a 50 percent increase in such actions when compared to the prior two years. The cases charged so far range from Russian procurement networks acquiring military-grade technology, to the theft of blueprints for sophisticated missile-detection technology in support of the People's Republic of China (PRC), to the smuggling of U.S.-origin items used in the production of unmanned aerial vehicles (UAVs) and ballistic missile systems to Iran. Just last month, for example, the work of the Strike Force led to charges against a Virginia company and two of its top executives for allegedly shipping sensitive U.S. electronics to Russia.

The Strike Force has employed an all-tools approach. In addition to our criminal cases, we imposed a nearly $6 million administrative penalty on a Pennsylvania company for shipping items to parties tied to China's hypersonics, UAV, and military electronics programs. We issued Temporary Denial Orders against nearly 30 entities (including airlines, freight forwarders, defense companies, and others) to cut off their access to controlled U.S. items. We worked with Treasury to add parties to their Specially Designated Nationals (SDN) list. And we nominated over 20 parties to the Entity List for their participation in the PRC's artificial intelligence (AI) and quantum technology programs.

At BIS, we've been laser-focused on countering the PRC's efforts to leverage advanced technologies for military modernization purposes. Last month, we imposed a half-million dollar administrative penalty on a New York company for shipping semiconductor materials to an Entity-Listed Chinese company. In October, a Chinese national pleaded guilty to illegally exporting semiconductor manufacturing equipment to company placed on the Entity List for its ties to the Chinese military. Over the past few years, we've brought numerous enforcement actions against Chinese procurement networks, including arresting a defendant in connection with an alleged plan to steal proprietary information related to AI technology from Google and obtaining a guilty plea from a NASA contractor who secretly funneled sensitive aeronautics software to an Entity-Listed Chinese university. In another case, we charged a Belgian national with crimes related to a years-long scheme to unlawfully export sensitive, military-grade technology to the PRC.

Our work has similarly led to the dismantling of over a dozen separate illicit Russian procurement networks, including one led by Maxim Marchenko, a Russian national who used several Hong Kong-based shell companies to obtain large quantities of sensitive, military-grade microelectronics. Marchenko was sentenced in July to three years in prison. We've also targeted Iranian procurement networks, including, most recently, arresting a dual U.S.-Iranian national charged with exporting U.S.-manufactured aircraft components to Iran and, separately, indicting a father-son duo who are alleged to have exported aerospace equipment to Iran.

(*Continued On The Following Column)

To further hone our prioritization efforts, we changed the categories of what we measure internally. More specifically, last fiscal year, we launched a new metrics initiative to track our investigative and analytic work, that is, to measure how close the fit is between our highest priorities and how we are spending most of our time. Now, for the first time ever, the annual performance plans for all of our managers include a component on how well their field office's investigations, or leads generated by their analysts, connect to our highest-priority areas. More specifically, we've internally identified items of greatest concern – like the disruptive technologies the Strike Force prioritizes; end users of greatest concern – like adversarial military, intelligence, and security agencies; and end uses of greatest concern – like WMD, military modernization efforts, and human rights abuses. We now track how many of our leads and cases are tied to one or more of these highest-priority areas. This way, we can better ensure that our agents and analysts are spending the bulk of their time where it can have the biggest impact. And it's working. Last year, we increased the percentage of our cases that involve a prioritized technology, end user, or end use from 70% to more than 85%, with over 95% of our leads tying to one or more of these categories as well.

We also strengthened our administrative enforcement program. We changed our procedures – to make our charging letters public when filed, to eliminate "no admit, no deny" settlements, and to raise the penalty amounts for serious violations. We clarified our voluntary self-disclosure policy to specify that if a company knows of a significant potential violation and affirmatively decides not to tell us, then that lack of disclosure will be an aggravating factor in any subsequent penalty calculation. A few months ago, we amended our administrative penalty and voluntary self-disclosure regulations to institutionalize these changes, and to give us more discretion in determining appropriate penalties for export control violations more broadly. We hired a first-ever Chief of Corporate Enforcement, to help advance our significant corporate investigations. And we made changes to our antiboycott enforcement program, where we re-ordered the regulatory penalty tiers, raised penalty amounts, eliminated "no admit, no deny" settlements, and announced an enhanced focus on foreign subsidiaries of U.S. companies.

These program and policy changes – designed to maximize our overall enforcement efforts – are bearing fruit. Over the last two years, we've had the agency's highest number ever of convictions, months of imprisonment, Temporary Denial Orders, end-use checks, and post-conviction denial orders. Last year, we imposed our largest standalone administrative penalty ever, $300 million, against Seagate for their shipment of millions of hard disk drives to Huawei. We also participated in the disruption of what is believed to be the world's largest-ever botnet, which infected over 19 million IP addresses and facilitated cyber-attacks, export violations, and billions of dollars of fraud.

(*Continued On The Following Page)

But it's not just the arrests, indictments, and administrative penalties. We've also publicly listed, for the first time ever, nearly 200 aircraft from Russia, Belarus, and Iran that have flown in violation of our controls and thus triggered General Prohibition 10 restrictions, which prohibit refueling, maintaining, or repairing those planes. And we've issued a record number of TDOs against the biggest airlines in Russia, Belarus, and Iran. Alongside DOJ, we seized a $13 million plane owned and operated for the benefit of Nicolás Maduro Moros and his regime in Venezuela. Our work also led to the forfeiture of a U.S.-manufactured Boeing 747 cargo plane, previously owned by Mahan Air, a sanctioned Iranian airline affiliated with the Islamic Revolutionary Guard Corps-Qods Force, a designated Foreign Terrorist Organization.

And that's not all. Beyond our casework, we've taken further prioritized actions. In the last three years, nominations from my team in Export Enforcement have resulted in over 900 parties from Russia, China, Iran, and elsewhere being added to the Entity List. This past fiscal year, for example, the team was responsible for adding over 320 parties to the Entity List and nearly 40 parties to the Unverified List. This represents an all-time high for Export Enforcement. We also – for the first time ever – placed 16 addresses in Hong Kong and Turkey on the Entity List for "housing" hundreds of shell companies responsible for more than $130 million in high-priority items being diverted to Russia. And we've also ensured that, under new regulations, persons blocked under certain OFAC sanctions programs are automatically subject to our controls as well.

Over the past three years, our aggressive and prioritized enforcement posture has become business as usual. It's our basic operating level. And I anticipate that you'll continue to see significant enforcement announcements in the weeks, months, and years to come.

Profile

Next, let me address our profile. I told the team on that first all-hands call that I would be a tireless champion for Export Enforcement and the work we do. Not just so that our agents, analysts, and Export Control Officers get the recognition they deserve, although that's important. But also because raising the profile of Export Enforcement out in the world has a strategic purpose. It acts as a force multiplier. Because we have such limited resources to meet such significant national security threats, we can't succeed by end-use checks and investigations alone. Those are essential, but they're not enough. We also need deterrence. We need to have industry fully committed to investing in robust compliance programs. And, my view, from the first day of my tenure, has been that one way to help make that happen is to continually evangelize about our work, including through speeches, interviews, conferences, and press releases. The goal is to let industry know that we want to partner with them to make sure they follow our rules (and also to let them know that there are meaningful consequences when they don't). By continuing to raise Export Enforcement's profile, we hope to convince companies to invest more heavily in compliance and prevention.

That's why I've agreed to speak at so many external events, including giving this keynote here today. Through webinars, podcasts, and conferences, I've spoken to thousands of trade practitioners and compliance professionals, C-Suite leaders, in-house and outside counsel, and trade associations. I've participated in panel discussions at forums as varied as the Munich Security Conference, the American Bar Association's White-Collar Crime Institute, and the American Bankers Association Financial Crimes Enforcement Conference. This speech marks the eighteenth formal speech that I've delivered to audiences around the globe – from New York to Singapore, from Texas to Toronto – about our national security mission and the critical importance of our work.

(*Continued On The Following Column)

And, of course, I haven't been the only government official out there speaking on this topic. The Secretary of Commerce, Gina Raimondo, has repeatedly emphasized the importance of export controls, explaining that, in the wrong hands, the most cutting-edge technology, like supercomputers or AI chips, can ultimately prove as deadly as any weapon. National Security Advisor Jake Sullivan has highlighted export controls' national security role, noting their centrality in helping the United States to maintain as large a scientific and technological lead as possible over our adversaries. Deputy Attorney General Lisa Monaco and other Department of Justice leaders have focused time and again on sanctions and export enforcement in their speeches, including by declaring sanctions and export enforcement a top Department of Justice corporate enforcement priority and noting how national security concerns must rise to the top of corporate compliance risk charts.

Three years after I told my team that we wanted to raise their profile, I submit that we've successfully done it. Industry and trade practitioners understand that we're now in a new era for export enforcement. Companies are evaluating their compliance programs to ensure they are robust and effective, lest they face multimillion dollar penalties for violating our rules. Word is out that export violations can no longer be considered just the cost of doing business. Instead, violations now present enterprise risk, which means that investment in compliance is crucial. The enhanced profile, combined with our voluntary self-disclosure policy changes, has led to a sharp rise in the number of significant disclosures we're receiving – an increase of nearly 70% when comparing the 18 month-period before and after the policy announcement.

I've heard several times at my speaking engagements over the past three years that I was the first speaker they ever had from the Commerce Department. I'll tell you how I responded: I may be the first, but I won't be the last. Export enforcement is now at the red-hot center of protecting our national security. Given our current geopolitical environment, that's likely to remain true for the foreseeable future. And so is our heightened profile.

Partnerships

Which leads me to the third and final "P" – partnerships: how we're working with our interagency partners to pool resources and authorities to bring enforcement actions; with our international counterparts to multilateralize our efforts; and with the private sector to help ensure compliance with our rules.

While the Disruptive Technology Strike Force is the highest-profile example of our interagency partnerships, it's certainly not the only one. We've also developed a close relationship with the Treasury Department, working with their Financial Crimes Enforcement Network (FinCEN) to publish – for the first time ever – a joint alert that created a new key term for financial institutions to use when filing Suspicious Activity Reports (SARs) for suspected Russian diversion. We then published two additional alerts together, creating a key term for export control evasion globally. To date, our analysts have reviewed over 1,400 SARs that contain one of these key terms, and we have been able to action more than 160 of those filings – either by sending a new lead to our enforcement agents, advancing an existing case, or developing an Entity List package. We've also built a close relationship with Treasury's Office of Foreign Assets Control (OFAC), with whose Director I have a standing biweekly coordination call. Last year, we signed an MOU formalizing our enhanced coordination and partnership. And, last April, we imposed a combined $3.3 million civil penalty against Microsoft to jointly resolve alleged violations of U.S. export controls and sanctions laws. You can expect to see additional coordinated enforcement actions from us in the near future.

(*Continued On The Following Page)

In addition to DOJ and Treasury, we've also worked with the interagency more broadly to publish an unprecedented number of advisory notes, guidance documents, and alerts. From the applicability of our controls to non-U.S. persons, to Iran's UAV-related activities, to the need for the transportation industry to "know their cargo," it's hard to find a topic where we haven't published something. It's unheard of for the government to release so many multi-agency guidance documents in such a short amount of time. That's a testament to our partners at the Departments of Justice, State, Homeland Security, and Treasury. And it reflects our core belief that we would much rather help industry understand and comply with our rules on the front end than pursue violations of them on the back end. When we're pursuing violations on the back end, it typically means the sensitive technology has already gone where it shouldn't and the national security harm has already happened.

Most recently, we partnered with the National Security Agency to build and deploy the Commerce Screening System (CSS), a brand-new game-changing information technology tool. Through the CSS, we are now able to screen every foreign party to a license application against certain intelligence holdings. Prior to the CSS, such screening was done manually, which meant that we were only able to screen about 800 license applications a year. Now, thanks to our new automated system, we'll be able to screen all of the approximately 40,000 applications that BIS receives annually. While the CSS just went live in October, it's already demonstrating real results. After two months of operation, this tool has enabled us to screen over 7,300 license applications and identify over 420 unique licenses where the intelligence holdings needed further review by a licensing officer prior to the licensing decision being made.

2. International partnerships

On the international front, while export controls have long been coordinated multilaterally on the policy side, there have not been any corresponding multilateral coordination mechanisms when it comes to enforcement. Thanks to our leadership efforts, and those of our allies and partners, I'm proud to say that's no longer the case. We've established – for the first time ever – three different enforcement coordination mechanisms.

First, we worked with the G7 to create a Sub-Working Group on Export Control Enforcement. The Sub-Working Group, established last year, provides the G7 countries and the European Commission a forum for exchanging information and operational results, discussing trends in research and analysis, and sharing best practices for enforcement. A few months ago, the G7 countries and the European Commission published, for the first time ever, joint guidance for industry on preventing evasion of the export controls and sanctions imposed on Russia.

Second, we established the Disruptive Technology Protection Network (DTPN) with the governments of Japan and South Korea, to expand information sharing and the exchange of best practices across the three countries' enforcement agencies. This past April, we held a high-level summit here in D.C. to formally launch the initiative, after it was first announced at the Trilateral Leaders' Summit at Camp David last summer. Since then, our teams have met regularly to exchange information, including just last week.

(*Continued On The Following Column)

And, third, we established the Export Enforcement Five, or E5, with the governments of Australia, Canada, New Zealand, and the United Kingdom. The E5 works with industry, including by publishing novel guidance, to harden supply chains of the items that Russia needs to sustain its unlawful full-scale invasion of Ukraine. The E5 also works to identify entities that have violated our coordinated export controls and to share investigative information for coordinated enforcement actions against them.

In addition to these unprecedented multilateral efforts, we've signed individual bilateral agreements for the first time with the European Anti-Fraud Office and with the Australian, Japanese, South Korean, and Swiss governments, to facilitate law enforcement cooperation and information sharing. We've also expanded our international footprint to better collaborate with partner governments across the globe. We now have 11 Export Control Officers in nine locations abroad, including two newly stationed in Taiwan and Finland. And, for the first time ever, we placed an enforcement analyst outside the United States, in Ottawa.

3. Private sector partnerships

Last but certainly not least, we've enhanced our partnerships with industry and academia. Over the past three years, we've conducted outreaches to nearly 6,000 companies, an all-time high, to ensure they're aware of regulatory changes and to warn them against illicit procurement attempts. We've issued supplier list and red flag letters, along with a guide explaining the difference between the two. In addition to our numerous multi-agency guidance documents, we also published BIS-specific recommendations for exporters on Russian evasion typologies, high-priority Harmonized System (HS) codes, and evasion red flags. Expanding beyond our more traditional stakeholders, we also recently published new BIS guidance for freight forwarders and for financial institutions containing best practice recommendations on how to avoid liability for export violations.

For academia, we launched the Academic Outreach Initiative to help universities protect their sensitive research from nation-state adversaries who seek to acquire it. The open and collaborative nature of our research institutions is fundamental to their success as science and technology leaders – but at the same time presents an inviting target for foreign adversaries who wish to exploit that environment and misappropriate those institutions' research. Over the last few years, we've doubled our reach – expanding the initiative from an initial 20 research institutions to 40, with 11 added this past October. For each of the 40 institutions, we've assigned a dedicated "Outreach Agent," a specific agent from their local BIS field office who meets with the institution regularly and serves as a resource and point of contact. We've also conducted webinars on identifying red flags for academia and other topics. And we published – for the first time ever – a compendium of resources to help universities comply with our export rules and an analysis of voluntary self-disclosure trends to help them identify high-risk areas.

(*Continued On The Following Page)

We've developed similar innovations to help industry comply with our antiboycott rules. We implemented a new data field to collect the names of foreign parties making boycott requests and then used that data to create – for the first time – a public list of such foreign parties. This innovative boycott Requester List now lets U.S. companies know which foreign parties have made boycott requests in the past – so that if they're dealing with those parties, they know to scrutinize transaction paperwork closely for reportable boycott requests. Beyond that, the Requester List has driven foreign parties to change their behavior by eliminating boycott language from their transaction documents, thus reducing boycott requests at their source. To date, over 20 companies have removed boycott-related language from their transaction documents. That benefits both U.S. companies and U.S. foreign policy interests.

As intended, these partnerships have worked as force multipliers. They've allowed us to galvanize resources across the interagency, across industry, and across the world to help protect sensitive technology from being misappropriated by our adversaries. The national security challenge we face is massive. Through prioritized enforcement efforts, an enhanced profile, and expanded partnerships, we're doing everything in our power to meet it.

So, I began my remarks by telling you about the "Steamboat Inspection" carving I see every day as I enter the Commerce Department. I want to close by telling you about a different part of what has been my daily commute for the past three years. Just before I arrive at work each morning, I drive down 14th Street through the National Mall. Each day, I take the conscious action of looking to my left, at the Washington Monument, and then to my right, at the United States Capitol. I do this intentionally to remind myself of the immense privilege I have been given – the privilege of serving the people of the United States, the privilege of waking up every day and driving to a job where the mission is to protect our national security by bringing to justice those who would transfer our country's most sensitive technology to our country's most serious adversaries.

It's been my deep and profound honor to serve as the Assistant Secretary for Export Enforcement these past three years. When this Administration began, I never could have predicted that this role would be the one I was asked to fill. But I am beyond fortunate to have had the opportunity to serve in it. The commitment, dedication, and impact of the men and women in Export Enforcement are second to none. It has been humbling to lead them and to learn from them. And while the time is rapidly approaching when I will no longer have the responsibility of leading them, I can't wait to see what they accomplish next.

Thank you.

****

Joint Statement from Foreign Ministers Condemning DPRK-Russia Cooperation

December 16, 2024

The text of the following statement was released by the Foreign Ministers of Australia, Canada, France, Germany, Italy, Japan, the Republic of Korea, New Zealand, the United Kingdom, the United States, and the High Representative of the European Union.

We, the Foreign Ministers of Australia, Canada, France, Germany, Italy, Japan, the Republic of Korea, New Zealand, the United Kingdom, the United States, and the High Representative of the European Union condemn in the strongest possible terms the increasing military cooperation between the Democratic People's Republic of Korea (DPRK) and the Russian Federation, including the deployment of DPRK troops to Russia for use on the battlefield against Ukraine. In a continued show of support and unity, we recall and reinforce our May 2024 coordinated sanctions action and joint statement on DPRK-Russia cooperation.

(*Continued On The Following Column)

Direct DPRK support for Russia's war of aggression against Ukraine marks a dangerous expansion of the conflict, with serious consequences for European and Indo-Pacific security. The DPRK's export of ballistic missiles, artillery shells, and other military materiel to Russia for use against Ukraine and Russia's training of DPRK soldiers involving arms or related materiel represent flagrant violations of United Nations Security Council resolutions 1718 (2006), 1874 (2009), and 2270 (2016). We are deeply concerned about any political, military, or economic support that Russia may be providing to the DPRK's illegal weapons programs, including weapons of mass destruction and their means of delivery, which would exacerbate the already tense environment on the Korean Peninsula.

Together, we reaffirm our unwavering commitment to support Ukraine as it defends its freedom, sovereignty, and territorial integrity. We urge the DPRK to cease immediately all assistance for Russia's war of aggression against Ukraine, including by withdrawing its troops. We urge Russia to immediately end its war of aggression against Ukraine and cease its military cooperation with the DPRK. We encourage members of the broader international community to join our call and we will continue to act in concert, including through imposition of economic sanctions, to respond to the danger posed by the DPRK-Russia partnership.

****

FOR IMMEDIATE RELEASE
Tuesday, December 10, 2024

Media Contact:
Office of Public Affairs, publicaffairs@doc.gov

Department of Commerce Awards CHIPS Incentives to Micron for Idaho and New York Projects and Announces Preliminary Memorandum of Terms for Virginia DRAM Project to Secure Domestic Supply of Legacy Memory Chips

CHIPS Award Will Support Micron's 20-year Manufacturing Vision to Expand Leading-Edge DRAM Production in Idaho and New York
CHIPS PMT Would Support Expansion of Virginia Facility to Onshore Important Memory Production

Today, the Biden-Harris Administration announced that the U.S. Department of Commerce awarded Micron Technology up to $6.165 billion in direct funding under the CHIPS Incentives Program's Funding Opportunity for Commercial Fabrication Facilities. The award follows the previously signed preliminary memorandum of terms, announced on April 25, 2024, and the completion of the Department's due diligence. This funding will support the first step in Micron's two-decade vision to invest approximately $100 billion in New York and $25 billion in Idaho, which will create approximately 20,000 jobs and will help the U.S. grow its share of advanced memory manufacturing from less than 2% today to approximately 10% by 2035. The Department will disburse the funds based on Micron's completion of project milestones.

This investment will help strengthen U.S. economic resiliency by bolstering a reliable domestic supply of leading-edge DRAM chips that are important components for advanced technologies such as, personal computing, industrial, high-performance compute, automotive, industrial, wireless communications and artificial intelligence. Micron's DRAM chips also power the company's performance memory, known as High-Bandwidth Memory (HBM), which is critical for enabling new AI models. With this funding, Micron plans to expand the development and production of the most advanced memory semiconductor technology in New York and Idaho and is committing to spend approximately $50 billion before the end of the decade.***(*Continued On The Following Page)***

In addition, the Biden-Harris Administration announced the Department of Commerce has signed a non-binding Preliminary Memorandum of Terms (PMT) with Micron Technology for up to $275 million in proposed funding to expand and modernize its facility in Manassas, Virginia. The expected capital expenditure for the modernization will be $2 billion over the next several years. The proposed project would onshore Micron's 1-alpha technology to its Manassas facility, significantly increasing monthly wafer output. Micron's 1-alpha node, an advanced DRAM process technology, offers meaningful improvements in bit density, power efficiency, and performance capability. Supporting a stable supply of Micron's 1-alpha technology would advance U.S. supply chain resiliency because the legacy DRAM memory chips that would be made in Virginia are important components for the automotive and industrial markets. Micron's proposed project in Manassas would be expected to create over 400 manufacturing jobs and up to 2700 community jobs at the peak of the project.

"Memory chips are foundational to all advanced technologies, and thanks to the bipartisan CHIPS and Science Act, America is rebuilding its capacity to produce these critical capabilities, said **U.S. Secretary of Commerce Gina Raimondo**. "With this investment in Micron, we are delivering on one of the core objectives of the CHIPS program – onshoring the development and production of the most advanced memory semiconductor technology, which is crucial for safeguarding our leadership on artificial intelligence and protecting our economic and national security."

"As the only U.S.-based manufacturer of memory, Micron is uniquely positioned to bring leading-edge memory manufacturing to the U.S., strengthening the country's technology leadership and fostering advanced innovation," said **Micron President and CEO Sanjay Mehrotra**. "Micron's investments in domestic semiconductor manufacturing capabilities, supported by the bipartisan CHIPS Act, will help drive economic growth and ensure that the U.S. remains at the forefront of technological advancements. We appreciate New York's Green CHIPS legislation and the local partnership with Micron to create a Community Investment Framework to revitalize central New York. Many federal, state and community leaders have played a pivotal role in the process, from the development of Micron's plans to finalizing essential investment tax credits. These include New York Governor Kathy Hochul, Senate Majority Leader Chuck Schumer, U.S. Senator Mark Warner, U.S. Senator Mike Crapo, U.S. Senator James Risch, Idaho Governor Brad Little, Virginia Governor Glenn Youngkin, Mayor Lauren McLean, and County Executive Ryan McMahon. Their contributions support Micron's continued industry leadership as we work to meet the growing demand for memory." For more information about Micron's award, please visit the CHIPS for America website.

As stated in the CHIPS Notice of Funding Opportunity for Commercial Fabrication Facilities, CHIPS for America will distribute direct funding to recipients for capital expenditures based on the completion of construction, technology, production, and commercial milestones. The program will track the performance of each CHIPS Incentives Award via financial and programmatic reports, in accordance with the award terms and conditions.
Additionally, as explained in its first Notice of Funding Opportunity, the Department of Commerce may offer applicants a PMT on a non-binding basis after satisfactory completion of the merit review of a full application. The PMT outlines key terms for a potential CHIPS incentives award, including the amount and form of the award. The award amounts are subject to due diligence and negotiation of award documents and are conditional on the achievement of certain milestones. After a PMT is signed, the Department of Commerce begins a comprehensive due diligence process on the proposed projects and continues negotiating or refining certain terms with the applicant. The terms contained in any final award documents may differ from the terms of the PMT being announced today.

About CHIPS for America
CHIPS for America has awarded over $25 billion of the over $36 billion in proposed incentives funding allocated to date. These announcements across 21 states are expected to create over 125,000 jobs. Since the beginning of the Biden-Harris Administration, semiconductor and electronics companies have announced over $450 billion in private investments, catalyzed in large part by public investment. CHIPS for America is part of President Biden and Vice President Harris's economic plan to invest in America, stimulate private sector investment, create good-paying jobs, make more in the United States, and revitalize communities left behind. CHIPS for America includes the CHIPS Program Office, responsible for manufacturing incentives, and the CHIPS Research and Development Office, responsible for R&D programs, that both sit within the National Institute of Standards and Technology (NIST) at the Department of Commerce. Visit chips.gov to learn more.

MISSION STATEMENT:

Given the geopolitical state of affairs with China, Russia, and Crimea, the Occupied territories of UKRAINE, Donetsk and Luhansk Oblast, embargoed countries and other specific threatening end users and entities, located in the United States and around the globe;

Evolutions in Business and the companies we serve, armed with robust compliance to the Export Administration Regulations, will adhere to best practices to protect our revenue and yours, and ensure the national security interests of the United States.

NOTE: In accordance with Title 17 U.S.C. Section 107, this material is distributed without profit or payment for non-profit news reporting and educational purposes only.

Evolutions in Business

Celebrating more than 30 Years

Keep up to date with latest trade news at:

www.eib.com

Check out our latest podcast:

https://www.buzzsprout.com/1592353/episodes/16248832