EIB World Trade Headlines

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

February 1, 2025 – Volume 20, Issue 3

FOR IMMEDIATE RELEASE January 13, 2025 BUREAU OF INDUSTRY AND SECURITY Office of Congressional and Public Affairs Media Contact: OCPA@bis.doc.gov

Biden-Harris Administration Announces Regulatory Framework for the Responsible Diffusion of Advanced Artificial Intelligence Technology New Framework Advances AI Innovation While Protecting U.S. National Security Washington, D.C. — Today, the Department of Commerce's Bureau of Industry and Security (BIS) announced controls on advanced computing chips and certain closed artificial intelligence (AI) model weights, alongside new license exceptions and updates to the Data Center Validated End User (VEU) authorization. This new regulation serves key U.S. national security and foreign policy interests and supports the Biden-Harris Administration's broader strategy to cultivate a secure and trusted technology ecosystem for the responsible use and diffusion of AI. "This policy will help build a trusted technology ecosystem around the world and allow us to protect against the national security risks associated with AI, while ensuring controls do not stifle innovation or US technological leadership," said U.S. Secretary of Commerce Gina Raimondo. "Managing these very real national security risks requires taking into account the evolution of AI technology, the capabilities of our adversaries, and the desire of our allies to share in the benefits of this technology. We've done that with this rule, and it will help safeguard the most advanced AI technology and help ensure it stays out of the hands of our foreign adversaries, while we continue to broadly share the benefits with partner countries." "The United States has a national security responsibility to preserve and extend American AI leadership, and to ensure that American AI can benefit people around the world. Today, we are announcing a rule that ensures frontier AI training infrastructure remains in the United States and closely allied countries, while also facilitating the diffusion of American AI globally," said National Security Advisor Jake Sullivan. "The rule both provides greater clarity to our international partners and to industry, and counters the serious circumvention and related national security risks posed by countries of concern and malicious actors who may seek to use the advanced American technologies against us."

"AI has been rapidly progressing over the last decade and will only grow more powerful, resulting in the emergence of highly capable models with significant dual-use applications," said Under Secretary of Commerce for Industry and Security Alan F. Estevez. "This rule will protect national security and advance U.S. foreign policy by ensuring the responsible diffusion of frontier AI technology across the world."

"Export controls provide a unique tool to address the quintessential dual-use nature of artificial intelligence," said Acting Assistant Secretary of Commerce for Export Administration Matthew Borman. "Through today's actions, we ensure the secure spread of AI capabilities, countering the potential for their use in weapons systems and other military activities contrary to U.S. national security. By doing so, we are creating paths that enable trusted partners to use this advanced technology for the benefit of civil society."

(*Continued On The Following Page)

NEWSLETTER NOTES

Over the past decade, AI models have shown striking performance improvements across many domains, giving everyday people increased access to tools that previously required specialized skills. As models continue to improve, this increased access will enable malicious actors to engage in activities that pose profound risks to U.S. national security and foreign policy, including enabling the development of chemical or biological weapons; supporting powerful offensive cyber operations; and further aiding human rights abuses, including mass surveillance. At the same time, AI has the potential to provide tremendous economic and social benefits to humanity. It is impossible to realize the full potential of those benefits without active participation from allies and partners – including like-minded nations, global firms, and research institutions committed to deploying U.S. technology essential to AI development under safe and secure conditions. The Biden-Harris Administration remains committed to ensuring that humanity can reap these critical benefits. Today's announcement seeks to keep advanced AI models out of the hands of malicious actors while also ensuring that secure and responsible foreign entities and destinations will have access to the most advanced U.S. AI models, and to the large clusters of advanced computing integrated circuits (ICs) necessary to train those models. Entities and destinations that are willing to abide by certain safety and security mitigations will receive access to AI models and large IC clusters. The framework adopts a three-pronged strategy. First, the rule updates controls for advanced computing chips by requiring authorizations for exports, reexports, and transfers (in-country) involving a broad set of additional countries. However, the rule also includes the following license exceptions and authorizations, which will ensure that commercial transactions that don't pose national security risks can proceed and the benefits of AI can be broadly shared:

- Exceptions for certain allies and partners: New License Exception Artificial Intelligence Authorization (AIA) allows for the export, reexport, or transfer (in-country) of advanced computing chips, without an authorization, to a set of allies and partners.
- Exceptions for supply chains: New License Exception Advanced Compute Manufacturing (ACM) allows for the export, reexport, or transfer (in-country) of advanced computing chips, without an authorization, for the purposes of development, production, and storage of these chips, except to arms-embargoed countries. This license exception builds on the Temporary General License from October 2023 rule to prevent disruption of supply chains.
- Low volume exception: New License Exception Low Processing Performance (LPP) allows limited amounts of compute to flow globally, except to arms-embargoed countries.
- Update to Data Center Validated End User (VEU) Program: The rule further bifurcates Data Center VEUs into: o Universal VEUs (UVEU): Provides U.S. and certain allied and partner country entities with the opportunity to obtain a single authorization that will allow the company to build data centers around the world without additional authorizations, except in arms-embargoed countries. o National VEUs (NVEU): Provides entities headquartered outside arms embargoed countries the opportunity to obtain an authorization that will allow the company to build data centers in specified locations without additional authorizations, except in arms-embargoed countries.

(*Continued On The Following Column)

When a license is required to export or reexport chips to a certain destination, license applications will be reviewed under a presumption of approval until the total quantity of controlled chips exported or reexported to that country exceeds a specified allocation. After a country reaches its allocation, applications will be reviewed under a policy of denial. Consistent with previously established policy, a presumption of denial remains in place for arms-embargoed countries, regardless of quantity. Authorized NVEUs will be able to build data centers up to a specified scale in each country. This allocation is separate from, and not impacted by, the host country's specified country allocation. Likewise, the low-volume orders are not affected by and do not count against country-level allocations. Authorized UVEUs will be required to keep at least 75% of their controlled advanced chips within the United States and certain allied and partner countries, and will be prohibited from installing more than 7% of their controlled chips in any single other country. U.S.-headquartered UVEUs will be required to keep at least 50% of their controlled advanced chips in the United States. Second, the rule institutes new controls on the model weights of the most advanced closed weight AI models. These controls will initially apply to the weights of models trained with 1026 computational operations or more, and authorizations will be required to export, reexport, or transfer (in-country) such weights to a broad set of countries. Additionally, the rule creates a new foreign direct product rule that applies these controls to certain model weights produced abroad using advanced computing chips made with U.S. technology or equipment. As with advanced computing chips, however, this rule includes several license exceptions for model weights:

Exception for deployments by U.S., ally and partner-headquartered entities: New License Exception Artificial Intelligence Authorization (AIA) allows for the export, reexport, or transfer (in-country) of otherwise controlled closed AI model weights, without an authorization, by companies headquartered in the United States and certain allies and partners, except to an arms-embargoed country.

- Exception for open models: Models with widely available model weights (i.e., open weight models) are not subject to controls. Additionally, the model weights of closed models that are less powerful than the most advanced open-weight models, even if they exceed the 1026 threshold, are not controlled. Third, BIS will impose security conditions to safeguard the storage of the most advanced models in destinations to protect U.S. national security and to mitigate the risk of diversion for advanced computing chips. Additional Information BIS's actions are taken under the authority of the Export Control Reform Act of 2018 and its implementing regulations, the Export Administration Regulations (EAR). Under these authorities, BIS possesses a variety of tools to control the export of U.S.-origin and certain foreign-produced commodities, software, and technology, as well as specific activities of U.S. persons, for national security and foreign policy reasons. For more information, please visit BIS's website at: https:www.bis.gov.

A Look Back at the Most Notable Cybersecurity Breaches in 2024

By Richard Roe and Scott Anderson

As we usher in 2025, Project Spectrum would like to take a moment to reflect on the past year. The headlines normally focus on the most sensational and impactful cyber-attacks, but what does not make the news are the 99.9% of cyber-attacks that are repelled by strong cybersecurity practices. As cyber defenders – we all must remember that and keep fighting the good fight to keep the bad guys at bay!

Without further ado, let's take a quick look back at the incidents that created headlines in 2024!

The 'Pervasives'

- ***China***

Throughout 2024, Salt Typhoon, a Chinese state-backed hacking group, executed a stealthy cyberespionage campaign targeting high-profile U.S. interests, including our critical infrastructure, and most recently, the Department of Treasury. One of their most prominent attacks targeted nine telecommunications companies – including behemoths Verizon and AT&T. Using advanced phishing attacks, the group infiltrated the telcos internal networks, planted persistent malware, and monitored communications over months with a specific eye on high-profile targets including government officials, campaign advisors, and corporate leaders involved in strategic technology and defense sectors. The attackers used custom-built malware that blended into legitimate traffic to evade detection. Once detected, the breach revealed vast quantities of exfiltrated data, potentially jeopardizing national security, and trade negotiations.

Salt Typhoon is just the most recent Chinese campaign to gain a foothold within the U.S. critical infrastructure, and it further exposed our systemic vulnerabilities. While the sophistication of nation state advanced persistent threats makes them difficult to stop, Salt Typhoon's success underscores the cyber defense community's collective need to implement zero-trust architecture to ensure the enforcement of strict access controls and continuous verification of network activity. It also reminds us that we must continue to build advanced threat intelligence sharing capabilities (particularly between the public and private sectors) to defray advanced cyber-attacks.

- ***Russia***

Like China, Russia is a formidable cyber adversary that leverages advanced capabilities when virtually targeting prominent U.S. institutions and organizations. One of the most prominent cyber-attacks this year – targeting Microsoft – was attributed to a Russian entity known as *Midnight Blizzard* (also referenced in some circles as *NEBELIUM*).

The September 2024 attack successfully breached the email accounts of high-ranking Microsoft executives. The attackers exploited vulnerabilities in email server configurations to gain access, stealing sensitive corporate communications and intellectual property. *Midnight Blizzard* stole and ultimately leaked emails revealing strategic discussions about product launches and geopolitical concerns tied to artificial intelligence development.

The success of this specific attack highlighted simple email vulnerabilities and demonstrated how Russian state-backed actors target intellectual property to gain economic and strategic advantages for their nation. The attack underscored the need for companies to implement end-to-end email encryption for any sensitive or proprietary electronic communications. It also demonstrated the need for organizations to flag any unusual activity in executive accounts.

(*Continued On The Following Column)

The fact that this was far reaching both geographically and across the entire sector highlighted the need for coordinated incident response planning among all like entities. This attack – effectively targeting disparate pieces that are part of the Internet of Things (IoT), underscored the need to better improve cybersecurity across that entire vast composition. This attack taught us that when it comes to health care, we need to be concerned about more than protecting Personally Identifiable Information (PII) – we also must ensure that network connected medical devices are properly protected.

- ***Change Healthcare***

Another prominent ransomware attack against the health care industry occurred in August when industry giant Change Healthcare was targeted by a group known as *ALPHV / BlackCat*. In conducting this exploit, attackers used a combination of social engineering techniques and advanced ransomware to encrypt vast amounts of patient data, including medical records, insurance claims, and payment details. Hospitals and clinics relying on Change Healthcare services experienced delays in patient care, with some forced to revert to manual operations. The company eventually paid a $22 million ransom, though recovery took weeks, leaving patients and providers scrambling to mitigate the fallout.

While this attack did not target medical devices (as the Ascension attack did) , the disruption was still significant and had life threatening implications. The incident further exposed the fragility of healthcare systems in the face of ransomware and that delays in treatment caused by such incidents can threaten patient well-being. To better defend in this space, the industry must learn from events like this and implement more advanced cybersecurity techniques including network segmentation and continuous monitoring. The incident also foot-stomped the collective need across the industry to maintain adequate cyber insurance coverage to expedite recovery.

The 'Blue Screen of Death'

In July 2024, cybersecurity firm CrowdStrike released a routine software update that inadvertently caused catastrophic disruptions to approximately 8.5 million Microsoft Windows systems worldwide. The update, meant to address minor vulnerabilities, introduced a severe compatibility issue with essential system drivers. Hospitals reported critical equipment failures, airlines grounded flights due to unresponsive scheduling systems, and financial institutions faced transaction delays and record-keeping errors. Times Square in New York City famously went dark for hours due to cascading effects in municipal power grids reliant on vulnerable systems. This single event triggered a ripple effect, disrupting global supply chains, emergency services, and day-to-day operations in over 70 countries.

This incident highlighted the vulnerability of critical infrastructure to software failures and demonstrated how a single update, even from a reputable cybersecurity firm, can have catastrophic global implications. Hindsight is always 20/20, but this incident was preventable. The key takeaways include the need for comprehensive testing of any updates before distributing them live. It also reminded all of the affected organizations that they need to have incident response plans at the ready, including the ability to quickly rollback to the previous baseline when an update goes awry.

(*Continued On The Following Column)

The Cascade

Hackers are now recognizing that one of the biggest force multipliers available to them is the breaching of 'Cloud Services' companies – enabling downstream access to multiple customers. In March 2024, hackers exploited weakly protected administrator credentials to breach Snowflake, a leading cloud data warehouse platform. The attackers gained unauthorized access to sensitive data belonging to high-profile Snowflake clients such as Ticketmaster, Santander Bank, AT&T, and many others. They downloaded vast data sets, including customer PII, transactional records, and proprietary business data. Investigations revealed that the breach was part of a coordinated attack leveraging phishing campaigns to gather credentials from third-party vendors integrated with Snowflake's platform.

This incident demonstrated the cascading risks of credential theft in cloud ecosystems, enabling access to many of the cloud clients. Like the CrowdStrike incident, this breach was preventable. The attackers exploited weak cybersecurity practices like poor password management and badly implemented privileged access practices. Simple use of strong multi-factor authentication techniques and internal implementation of least-privilege principles would have prevented this unauthorized access and ultimate exploitation of the laundry list of Snowflake customers. The incident also reminds us that companies must always assess the cybersecurity practices of third-party vendors before integrating them into their ecosystems.

The One from 2023

Beginning in April 2024 and rolling through the summer months, hackers exposed volumes of stolen data from National Public Data on the Dark Web. While the data was not exposed publicly until 2024, the exploit that enabled the theft actually occurred in December 2023.

This breach exposed background check information of over 1.3 million individuals – and also resulted in the theft of social security numbers, employment histories, and legal records. The breach occurred due to a poorly protected cloud database that had no encryption and required no authentication. This incident exposed systemic lapses in protecting personal data in large organizations and highlighted the real-world consequences of negligence in database management. As with most cybersecurity breaches, this was entirely preventable. Simple use of data encryption tools and techniques and the implementation of authentication protocols would have prevented this unauthorized access.

The Last Word

As we mentioned initially, despite that recounting, the news is not all bad! The organizations that practice strong cybersecurity far outnumber those that do not – and as a whole – we are learning valuable lessons from incidents like those outlined herein so we improve our overall cyber hygiene and make the attackers jobs that much more difficult. If breaches number in the millions – attacks successfully defrayed reach the billions, but that still is not good enough and we have to strive for perfection.

Project Spectrum recognizes our vast responsibility to do our part to help each of you defend your critical piece of the defense community. If you have not leveraged us in the past – make it your top resolution of 2025! Here is to a cybersecure 2025!

Happy New Year from the Project Spectrum Team

FOR IMMEDIATE RELEASE
Tuesday, January 14, 2025

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

United States and Norway Issue Innovative Report Creating Greater Transparency in Critical Mineral Supply Chains

WASHINGTON – Today, the U.S. Department of Commerce and the Norwegian Ministry of Trade, Industry, and Fisheries issued a thorough, innovative report presenting our shared understanding of non-market policies and practices (NMPPs) of certain third-party countries that may distort critical mineral markets ("NMPP Report"). The NMPP Report marks an important milestone in the United States and Norway's pursuit of sustainable, high-standard, market-oriented critical mineral mining and processing activities globally.

The International Trade Administration's Industry and Analysis business unit played a leading role in the development of this report. "Securing our critical mineral supply chains is vital to protecting our national security and enhancing our economic competitiveness," **said Assistant Secretary of Commerce for Industry and Analysis Grant Harris.** "This report provides an in-depth analysis of how non-market policies and practices have impacted the markets for critical minerals. It should be used to inform actions by market-oriented economies and industry partners to differentiate markets and strengthen these vital supply chains."

The NMPP Report provides an overview of mineral supply chains in the United States and Norway and NMPPs impacting mineral markets, and an examination of how these NMPPs have been employed in the supply chains for rare earth elements, graphite, cobalt, nickel, and magnesium and impacted the markets of these minerals.

The Report finds that, absent action by market-oriented countries, in partnership with industry and other stakeholders, critical mineral supply chains are likely to remain vulnerable. This Report can be used to identify appropriate responses to NMPPs, advancing the long-term commercial viability of sustainable, high-standard market-oriented critical minerals and processing activities in the United States, Norway, and globally.

The NMPP report is available here.

****

Implementation of Additional Due Diligence Measures for Advanced Computing Integrated Circuits; Amendments and Clarifications; and Extension of Comment Period

Publication date: 1/16/2025
End of Comment Period: 3/14/2025

Link here:
https://www.federalregister.gov/documents/2025/01/16/2025-00711/implementation-of-additional-due-diligence-measures-for-advanced-computing-integrated-circuits

****

Department of Commerce Advocacy Center Launches Expanded Support for U.S. Companies Competing Abroad

FOR IMMEDIATE RELEASE
Friday, January 10, 2025

Office of Public Affairs

publicaffairs@doc.gov

WASHINGTON – Today, the U.S. Department of Commerce announced an expansion of its support for U.S. companies competing for major investment and concession projects in other countries. Responding to growing competition from strategic adversaries in foreign markets and industry demand for additional tools to counter unfair foreign competition, this initiative aims to broaden the Department's Advocacy Center services. The expansion is designed to help eligible U.S. businesses competing to secure contracts in major foreign government investment and concession projects in critical sectors like energy, infrastructure, and critical minerals and metals mining that will benefit the U.S. economy.

"This project represents a bold new step in how the Department of Commerce levels the playing field for U.S. businesses and strengthens American leadership worldwide, underscoring what I've long contended: economic security is national security," said U.S. Secretary of Commerce Gina Raimondo. "In taking this step, we're directly responding to needs U.S. companies have raised in a way that's consistent with our strategic priorities, drawing countries and partners around the world closer to the United States by strengthening our commercial ties. Helping U.S. companies win overseas means economic benefits back home — more jobs, a stronger industrial base, and more secure and resilient supply chains."

Since its inception in 1993, the Advocacy Center has successfully coordinated U.S. government efforts to help American companies secure major foreign government procurement contracts and fairly compete against international rivals. These efforts are critical for driving export-led economic growth. In Fiscal Year 2024 alone, the Advocacy Center helped U.S. companies win contracts worth $72.6 billion, supporting an estimated 300,000 U.S. jobs.

(*Continued On The Following Column)

This new approach underscores the Biden-Harris Administration's commitment to fostering new opportunities for American businesses in sectors critical to global economic development. By providing expanded advocacy services, the Department of Commerce's Advocacy Center aims to bolster U.S. competitiveness abroad, increase export opportunities, and better position American firms to thrive in a dynamic international market.

About the Advocacy Center: The U.S. Department of Commerce Advocacy Center serves as the central point for coordinating U.S. government efforts to promote American companies competing for international contracts. By working closely with U.S. diplomatic missions and federal agencies, the Advocacy Center helps U.S. businesses receive the support they need to compete fairly and win foreign project or procurement opportunities worldwide. For more information, visit trade.gov/advocacy

About the International Trade Administration: The International Trade Administration (ITA) at the U.S. Department of Commerce is the premier U.S. Government resource for American companies competing in the global marketplace. Operating in more than 100 U.S. locations and 80 markets worldwide, ITA promotes trade and investment, assists U.S. businesses and workers to export and expand globally, and ensures fair trade and compliance by enforcing U.S. trade laws and agreements. For more information on ITA, visit trade.gov.

****

FOR IMMEDIATE RELEASE
Wednesday, January 16, 2025

Media Contact:
Office of Public Affairs, publicaffairs@doc.gov
Department of Commerce Announces Preliminary Terms with Analog Devices, Coherent Corp., Intelligent Epitaxy Technology, Inc. and Sumika Semiconductor Materials Texas Inc., to Strengthen U.S. Semiconductor Leadership

Proposed CHIPS Investments in Massachusetts, Oregon, Washington, Pennsylvania, and Texas, would Advance Key Semiconductor Technologies Capabilities to Support U.S. Economic and National Security

Today, the U.S. Department of Commerce announced the signing of four separate non-binding preliminary memoranda of terms (PMT) under the CHIPS and Science Act to provide up to $105 million in proposed direct funding to Analog Devices, Inc. ("ADI"), up to $79 million in proposed direct funding to Coherent, up to $10.3 million in proposed direct funding to Intelligent Epitaxy Technology, Inc. ("IntelliEPI), and up to $52.1 million in proposed direct funding to Sumika Semiconductor Materials Texas Inc., ("Sumika"). The proposed investment in ADI would support the expansion and modernization of two advanced research & development (R&D) and Radio Frequency (RF) Microwave (MW) systems manufacturing facilities in Chelmsford, Massachusetts, as well as expand and modernize two semiconductor fabrication facilities in Beaverton, Oregon and Camas, Washington which could create up to an estimated 500 manufacturing and engineering jobs across all sites with proposed CHIPS funding. The proposed investment in IntelliEPI would support the expansion and modernization of it's existing manufacturing facility in Allen, Texas to increase production of epitaxial wafers and could create 40 manufacturing jobs and 16 construction jobs. The proposed investment in Coherent would support the expansion of it's existing manufacturing facility in Easton, Pennsylvania and would create approximately 360 jobs. The proposed investment in Sumika would support the construction of a greenfield factory in Baytown, Texas to manufacture high-purity chemicals and could create over 290 jobs.

"Thanks to the bipartisan CHIPS and Science Act, we are making targeted investments up and down the semiconductor supply chain to revitalize semiconductor manufacturing in the United States and advance U.S. economic and national security," said **U.S. Secretary of Commerce Gina Raimondo**. "The proposed investments we're announcing today would support projects that will bolster semiconductor and materials production across the country and advance America's technological leadership on the world stage."
The proposed funding announced today would support the following projects:

(*Continued On The Following Column)

- **ADI (Chelmsford, Massachusetts; Beaverton, Oregon; Camas, Washington):** The Department of Commerce's proposed investment of up to $105 million would support the company's projects in Massachusetts and the Pacific Northwest. The investment in Massachusetts would enable the company to increase module production output for its packaging and test facility, which would expand capacity for commercial, space, and defense applications as well as new commercial phased array antenna and sensor solutions. CHIPS for America's proposed investment in Oregon and Washington would support the expansion of front-end mature node semiconductor manufacturing for devices used in a wide variety of applications, including but not limited to automotive, industrial, and defense applications. The proposed funding for the Oregon and Washington project also aims to increase capacity at the facilities by 70% across a variety of mature node processes, including onshoring 180nm and 350nm process nodes important to diverse end markets. As part of this modernization, ADI would undertake efforts to reduce the use of solvents at its Oregon and Washington facilities using state-of-the-art processes which are more environmentally friendly. To advance the company's workforce efforts and community investments, ADI plans to build on its partnerships with local universities, community colleges, and other education partners. As part of the Oregon and Washington project, ADI has launched the Semiconductor Advanced Manufacturing Upskilling (SAMU) technician training facility, which will offer programs to support manufacturers and collaborators in the Silicon Forest. ADI also plans to provide additional financial support for manufacturing employees to achieve associate degrees and technical certifications.

Coherent (Easton, Pennsylvania): The Department of Commerce's proposed investment of up to $79 million would support the expansion of Coherent's existing manufacturing facility in Easton, Pennsylvania to increase production capacity of 150mm and 200mm silicon carbide (SiC) substrates. The proposed CHIPS investment would also support the expansion of the facility's SiC epitaxial wafer manufacturing capacity, back-end of line processing, electronic performance, and reliability testing capabilities. SiC substrates are an important bandgap material with end uses in energy and military applications. CHIPS for America's proposed investment to expand Coherent's production capacity in Easton could increase its substrate capacity by over 750,000 substrates per year and more than double the output of epitaxial wafersper year. The proposed project is expected to create 320 manufacturing jobs and 40 construction jobs.

IntelliEPI (Allen, Texas): The Department of Commerce's proposed investment of up to $10.3 million would support the expansion and modernization of IntelliEPI's existing manufacturing facility in Allen, Texas. IntelliEPI is a leading provider of epitaxy wafers for advanced compound semiconductor applications. The company specializes in the growth of high-quality epitaxy material on Indium Phosphide ("InP"), Gallium Arsenide ("GaAs"), Gallium Antimonide ("GaSb"), and Gallium Nitride ("GaN") compound semiconductor wafers based on an advanced production Molecular Beam Epitaxy (MBE) technology platform. IntelliEPI serves a global clientele in markets spanning defense, AI/datacenters, telecommunications, automotive, and more. Through this proposed investment, CHIPS for America could strengthen the U.S. semiconductor supply chain by expanding domestic capacity for epitaxy wafers. This proposed project is expected to create 40 manufacturing jobs and 16 construction jobs.

(*Continued On The Following Page)

- **Sumika (Baytown, Texas):** The Department of Commerce's proposed investment of up to $52.1 million would support the construction of a greenfield factory in Baytown, Texas to manufacture ultra-high purity (UHP) isopropyl alcohol (IPA) used in advanced logic and memory chip production. Sumika is a subsidiary of the Japan-based Sumitomo Chemical Co., LTD, the largest global producer of high-purity chemicals for the semiconductor industry. The proposed investment represents the company's first major investment in high-purity chemicals production in the U.S. UHP IPA production is almost entirely concentrated in East Asia. Through this proposed investment, CHIPS for America would strengthen the U.S. semiconductor supply chain by ensuring a domestic supply of this key semiconductor manufacturing components and reducing risk involved in shipping UHP IPA across the globe. To advance its local workforce efforts, Sumika has partnered with the Lee College Center for Workforce and Community Development and San Jacinto College with the goal of structuring classes or new curriculum units to educate and train students in high purity chemical processing. The proposed project is expected to create 43 manufacturing jobs and 250 construction jobs.

"ADI is at the forefront of innovation in the expansion of U.S. semiconductor manufacturing," said **Vincent Roche, CEO and Chair at Analog Devices**. "Our focus on enabling innovation at the Intelligent Edge is driving advancements in process technologies that are critical to our global customer base. This investment will help us strengthen our workforce training and community partnerships, as well as expand our efforts to manage our environmental footprint."
"We are deeply honored to partner with the U.S. Department of Commerce under the CHIPS and Science Act to support the growth of critical silicon carbide infrastructure here in the U.S," said **Rob Beard, Chief Legal and Global Affairs Officer for Coherent**. "This proposed investment reflects a shared commitment to strengthening domestic manufacturing, advancing cutting-edge technologies, and creating high-quality jobs in Pennsylvania. By expanding our production capabilities for silicon carbide substrates and epitaxial wafers, Coherent is poised to drive innovation and meet the growing demand for materials that power energy and advanced applications."
ADI and Coherent 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.

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 proposed amount and form of the award. The proposed 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.

(*Continued On The Following Column)

About CHIPS for America

CHIPS for America has awarded over $33 billion of the over $36 billion in proposed incentives funding allocated to date. These announcements across 22 states are expected to create over 125,000 jobs. Since the beginning of the Biden-Harris Administration, semiconductor and electronics companies have announced nearly $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
January 17, 2025
www.bis.gov

BUREAU OF INDUSTRY AND SECURITY
Office of Congressional and Public Affairs
OCPA@bis.doc.gov

Haas Automation to Pay Over $2.5 Million in Combined Civil Penalties to BIS and OFAC for Prohibited Transactions, Including with Entities Affiliated with Chinese and Russian Defense Sectors

WASHINGTON, D.C. — Today, as part of a coordinated enforcement effort, the Department of Commerce's Bureau of Industry and Security (BIS) and the Department of the Treasury's Office of Foreign Assets Control (OFAC) imposed approximately $2.5 million in combined civil penalties against Haas Automation, Inc. (Haas) for alleged and apparent violations of U.S. export controls and sanctions laws, including illegal shipments of Computer Numerical Control (CNC) machine parts to Entity-Listed parties in Russia and China. The transactions charged by BIS involved parties that were added to the Entity List for supporting the defense sectors of China or Russia.

As part of a settlement agreement with Haas, BIS issued an order imposing an administrative penalty of $1.5 million, as well as an ongoing audit and reporting requirement. In addition to the BIS penalty, Haas entered a corresponding settlement with OFAC whereby Haas agreed to a $1,044,781 civil penalty to resolve apparent violations of OFAC's sanctions regulations involving Russia and Ukraine.

"Today's coordinated resolution with OFAC demonstrates our resolve to hold accountable companies that do not put in place effective compliance programs to prevent exports to Entity Listed companies," said **Acting Assistant Secretary for Export Enforcement Kevin J. Kurland**. "That's especially true when parties on the Entity List have ties to China's or Russia's destabilizing military modernization programs."

(*Continued On The Following Page)

Under the terms of the BIS Settlement Agreement, Haas admitted to 41 violations of the Export Administration Regulations (EAR) involving sales to Entity-Listed parties in China and Russia without BIS authorization. The relevant sales parts used to service previously sold Haas CNC machines—were valued in total at approximately $29,254 and were used to service CNC machines worth far more. Haas also admitted to an additional violation involving the filing of inaccurate Electronic Export Information (EEI) for certain shipments to Russia. Haas cooperated with the investigation by BIS's Office of Export Enforcement (OEE) Los Angeles Field Office and OFAC, and took remedial measures after discovering the conduct, which resulted in a reduction of the penalty.

"Exporting items to Entity-Listed parties in Russia and China has serious national security implications," said **OEE Director John Sonderman**. "When choosing to do business in these jurisdictions, industry must enhance screening efforts when it comes to prohibited parties."

Headquartered in Oxnard, California, Haas is a privately held manufacturer of machine tools and related parts, including CNC vertical and horizontal machining centers and CNC lathes. CNC machines and parts have a wide range of potential applications, including uses across the electronics, transportation, oil and gas, aerospace, marine, and military and defense industries.

On 32 occasions between April 2019 and March 2024, Haas violated the EAR by selling CNC machine parts designated as EAR99, through Haas's authorized distributors, for export, reexport, or transfer (in-country) to defense sector parties that were on the BIS Entity List in China, including Beijing University of Aeronautics and Astronautics (also known as Beihang University), Shandong Institute of Space Electronic Technology, and China Electronics Technology Group Corporation 14th Research Institute (CETC 14). Additionally, Haas violated the EAR by making nine sales to two defense sector parties on the Entity List in Russia—DJSC Factory Krasnoe Znamya and JSC LEMZ R&P Corporation—between January 2020 and November 2021.

The full order, settlement agreement, and Proposed Charging Letter are available online here.

Additional Information:
BIS actions are taken under the authority of the Export Control Reform Act of 2018 (ECRA, 50 U.S.C. §§ 4801-4852) and its implementing regulations, the EAR. BIS controls exports of dual-use commodities, technology, and software for reasons of national security, missile technology, nuclear non-proliferation, chemical and biological non-proliferation, crime control, and regional stability. Criminal and administrative sanctions can be imposed for violations of the EAR. Under ECRA, among possible administrative sanctions, civil monetary penalties can reach up to $374,474 per violation or twice the value of the transaction, whichever is greater. For more information, please visit https://www.bis.gov/enforcement.

Report suspected export control violations through the BIS online tip portal. You can also call the Enforcement Hotline at 1-800-424-2980 or email EELead@bis.doc.gov.

NEWER REGULATIONS EAR

§ 743.2 High performance computers: Post shipment verification reporting.

(a) *Scope.* This section outlines special post-shipment reporting requirements for exports of certain computers to destinations in Computer Tier 3, see § 740.7(d) for a list of these destinations. Post-shipment reports must be submitted in accordance with the provisions of this section, and all relevant records of such exports must be kept in accordance with part 762 of the EAR.

(b) *Requirement.* Exporters must file post-shipment reports and keep records in accordance with recordkeeping requirements in part 762 of the EAR for high performance computer exports to destinations in Computer Tier 3, as well as, *exports of commodities used to enhance computers* previously exported or reexported to Computer Tier 3 destinations, where the "Adjusted Peak Performance" ("APP") is greater than that listed in ECCN 4A003.b in the Commerce Control List, supplement no. 1 to part 774 of the EAR.

(c) *Information that must be included in each post-shipment report.* No later than the last day of the month following the month in which the export takes place, the exporter must submit the following information to BIS at the address listed in paragraph (d) of this section:

(1) Exporter name, address, and telephone number;
(2) License number;
(3) Date of export;
(4) End-user name, point of contact, address, telephone number;
(5) Carrier;
(6) Air waybill or bill of lading number;
(7) Commodity description, quantities—listed by model numbers, serial numbers, and APP level in WT; and
(8) Certification line for exporters to sign and date. The exporter must certify that the information contained in the report is accurate to the best of his or her knowledge.

Note to paragraph (c) of this section:
Exporters are required to provide the PRC End-User Certificate Number to BIS as part of their post-shipment report. When providing the PRC End-User Certificate Number to BIS, you must identify the transaction in the post shipment report to which that PRC End-User Certificate Number applies.

(d) *Address.* A copy of the post-shipment report(s) required under paragraph (b) of this section shall be delivered, via courier, to: U.S. Department of Commerce, Office of Enforcement Analysis, HPC Team, 14th Street and Constitution Ave., NW., Room 4065, Washington, DC 20230. Note that BIS will not accept reports sent C.O.D.

[71 FR 20886, Apr. 24, 2006, as amended at 73 FR 35, Jan. 2, 2008; 76 FR 36988, June 24, 2011; 77 FR 39369, July 2, 2012; 79 FR 45296, Aug. 4, 2014; 81 FR 64675, Sept. 20, 2016]

Secretary Rubio's Meeting with Indian External Affairs Minister Jaishankar

January 21, 2025

The below is attributable to Spokesperson Tammy Bruce:

Secretary of State Marco Rubio met with Indian External Affairs Minister Subrahmanyam Jaishankar today in Washington, D.C. Secretary Rubio and External Affairs Minister Jaishankar affirmed a shared commitment to continuing to strengthen the partnership between the United States and India. They discussed a wide range of topics, including regional issues and opportunities to further deepen the U.S.-India relationship, in particular on critical and emerging technologies, defense cooperation, energy, and on advancing a free and open Indo-Pacific region. Secretary Rubio also emphasized the Trump Administration's desire to work with India to advance economic ties and address concerns related to irregular migration.

****

Secretary Rubio's Meeting with Japanese Foreign Minister Iwaya

01/21/2025 11:05 PM EST

Office of the Spokesperson

The below is attributable to Spokesperson Tammy Bruce:
Secretary of State Marco Rubio met today with Japanese Foreign Minister Iwaya Takeshi in Washington. They discussed plans to deepen ties during the Trump Administration, and how the United States and Japan can work together to counter ongoing threats in the Indo-Pacific and around the world, including joint efforts against China's destabilizing actions. The two also discussed concerns over both the DPRK's political and security alignment with Russia, as well as China's support for Russia's defense industrial base. Secretary Rubio underscored enduring U.S. commitment to the U.S.-Japan Alliance as the cornerstone of security and prosperity in the region.

****

Release of Galaxy Leader Crew Members

01/23/2025 12:54 PM EST

Office of the Spokesperson
Today, we welcome the long-overdue release of 25 crew members of the MV Galaxy Leader hailing from Bulgaria, Mexico, the Philippines, Romania, and Ukraine. The United States is deeply grateful to the Sultanate of Oman for its essential and timely efforts to secure the release of the crew.

The Houthis had unlawfully detained the crew since violently seizing their vessel over a year ago. The Houthis have still not released the MV Galaxy Leader itself, which is stolen property. Houthi attacks have endangered the lives of seafarers, hindered the delivery of essential humanitarian assistance, and harmed economies across the region.

We must not be distracted by this insufficient action by the Houthis. Within Yemen, the Houthis continue to round up and detain hundreds of local staff members of the UN, NGOs, and diplomatic missions under abysmal conditions, including dozens of current and former Yemeni staff of the United States government unlawfully held based on false accusations. The Houthis have also stated that they will continue their unlawful attacks in the Red Sea against certain vessels associated with Israel. The Houthis must permanently cease all attacks in the Red Sea and surrounding waterways without exception and immediately release all of the hundreds of detainees.

****

India Republic Day

01/25/2025 05:00 PM EST

Marco Rubio, Secretary of State
On behalf of the United States of America, I congratulate the people of India as they celebrate their nation's Republic Day. As they commemorate the adoption of the Constitution of India, we join them in recognizing its enduring significance as the foundation of the world's largest democracy.

The partnership between the United States and India continues to reach new heights and will be a defining relationship of the 21st century. The enduring friendship between our two peoples is the bedrock of our cooperation and propels us forward as we realize the tremendous potential of our economic relationship. We look forward to deepening our cooperation in the year ahead, including by advancing our joint efforts in space research and coordination within the Quad to promote a free, open, and prosperous Indo-Pacific region.

****

New entry requirements for U.S. Citizens traveling or transiting through United Kingdom airports

Since January 8, 2025, U.S. citizens traveling to the United Kingdom for short visits, tourism, or business, including those just passing through UK airports, will need an Electronic Travel Authorization (ETA) if they do not have a UK visa or legal residency in the UK or the Republic of Ireland. This requirement applies to all parts of the UK, including Northern Ireland and British Overseas Territories. The ETA is similar to the U.S. ESTA system and acts as a pre-clearance for travel. This change is part of the UK's move towards a digital border system.

An Electronic Travel Authorization (ETA):

- May take up to three working days to process.
- Costs £10 ($12.75).
- Is required for travelers of all ages.
- Is valid for two years or the remaining period of validity on a passport, whichever is shorter;
- Does not require travel details.

One does not need an ETA if they already have a visa, an exempt vignette, or have a British or Irish passport. Other nationalities that ordinarily require a visa to visit the UK will continue to do so and should not obtain an ETA.

https://www.gov.uk/guidance/apply-for-an-electronic-travel-authorisation-eta

Restoring a Tough U.S.-Cuba Policy

01/31/2025 06:51 PM EST

Marco Rubio, Secretary of State
Within the first two weeks of President Trump's term, the State Department took decisive action to rescind major last-minute policy changes on Cuba announced by the previous administration on January 14.

The President acted on his first day in office to keep Cuba on the SST list, where it belongs. The Cuban regime has long supported acts of international terrorism. We call for the regime to end its support for terrorism, and to stop providing food, housing, and medical care to foreign murderers, bombmakers, and hijackers, while Cubans go hungry and lack access to basic medicine.

In a January 29 letter to the appropriate Congressional committees, I withdrew the prior administration's letter regarding the LIBERTAD Act. The Trump Administration is committed to U.S. persons having the ability to bring private rights of action involving trafficked property confiscated by the Cuban regime.

On January 31, I approved the re-creation of the Cuba Restricted List, which prohibits certain transactions with companies under the control of, or acting for or on behalf of, the repressive Cuban military, intelligence, or security services or personnel. The State Department is re-issuing the Cuba Restricted List to deny resources to the very branches of the Cuban regime that directly oppress and surveil the Cuban people while controlling large swaths of the country's economy. In addition to restoring the entities that were on the list until the final week of the previous administration, we are adding Orbit, S.A., a remittance-processing company operating for or on behalf of the Cuban military.

The State Department promotes accountability for the Cuban regime for oppressing its people and rejects Cuba's malign interference across the Americas and throughout the world. We support the Cuban people's human rights and fundamental freedoms and demand the release of all unjustly detained political prisoners. Our Embassy in Havana is meeting with families of those unjustly detained, as well as dissidents, so that they know the United States wholeheartedly supports them. We are steadfast in our commitment to the Cuban people and promote accountability for the Cuban regime's actions.

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.

Keep up to date with latest trade news at:

www.eib.com

Check out our latest podcast:
NATO 75th Anniversary Summit Review

https://www.buzzsprout.com/1592353/15500353