EIB World Trade Headlines

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

May 15, 2023 - Volume 18, Issue 10

Commerce Department starts process to fund tech hubs across the US with $500 million in grants

By JOSH BOAK The Associated Press, Updated May 12, 2023, 5:48 a.m.

"This is about taking these places on the edge of glory to being world leaders," Commerce Secretary Gina Raimondo told The Associated Press. "My job is to enhance America's competitiveness. "Evan Vucci/Associated Press

WASHINGTON — The Commerce Department on Friday is launching the application process for cities to receive a total of $500 million in grants to become technology hubs.

The $500 million is part of a $10 billion authorization from last year's CHIPS and Science Act to stimulate investments in new technologies such as artificial intelligence, quantum computing and biotech. It's an attempt to expand tech investment that is largely concentrated around a few US cities — Austin, Texas; Boston; New York; San Francisco; and Seattle — to the rest of the country.

"This is about taking these places on the edge of glory to being world leaders," Commerce Secretary Gina Raimondo told The Associated Press. "My job is to enhance America's competitiveness."

The Biden administration has made it a priority to set an industrial strategy of directing government investment into computer chips, clean energy and a range of other technologies. Officials say that being leaders in those fields will foster economic and national security, reflecting a belief that the best way to compete against China's ascendance will come from building internal strength.

The tech hubs are meant to build up areas that already have major research specialties but lack the access to financing that could fuel stronger growth and business formation in those fields. Pockets of the US already have leading-edge tech such as medical devices in Minnesota, robotics in Pittsburgh and agricultural technology in Fresno, California. But the challenge has been finding ways to boost those fields so that government investment leads to more support from private capital.

To qualify for the tech hub money, each applicant will need a partnership that includes one or more companies, a state development agency, worker training programs, a university and state and local government leaders. Roughly 20 cities are expected to be designated as tech hubs with 10 eventually receiving funding.

President Joe Biden hopes to broaden the funding over time, requesting in his budget proposal that Congress appropriate another $4 billion for it over the next two years. Raimondo said that she expects a large number of applications from across the political spectrum.

The tech hubs program, formally the Regional Technology and Innovation Hub Program, ties into a political message that Biden has delivered in speeches. The Democratic president has said that people should not feel forced to leave their hometowns to find good jobs nor should opportunity cluster in just a few parts of the country while other regions struggle.

"You shouldn't have to move to Silicon Valley if you're a scientist with a great idea," Raimondo said.

NEWSLETTER NOTES

Department of Justice
Office of Public Affairs
FOR IMMEDIATE RELEASE
Thursday, May 11, 2023

Justice Department Seizes 13 Domains Used by Lebanese Hezbollah and its Affiliates

The Justice Department today announced the seizure of 13 domains used by Specially Designated Nationals (SNDs), Specially Designated Global Terrorists (SDGTs), and their members associated with Lebanese Hezbollah.

According to court records, the United States obtained court authorization to seize five domains registered to the Public Interest Registry (PIR) – moqawama.org, almanarnews.org, manarnews.org, almanar-tv.org, and alshahid.org – and eight domains registered to Verisign Inc. – manartv.net, manarnews.net, almanar-tv.com, almanar-tv.net, alidaamouch.com, Ibrahim-alsayed.net, alemdad.net, and naimkassem.net.

"Today's web domain seizures deny terrorist organizations and affiliates significant sources of support and makes clear we will not allow these groups to use U.S. infrastructure to threaten the American people," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "The Justice Department will continue to enforce economic sanctions as part of our commitment to deploy all available tools against threats from hostile nation-states and terrorist actors alike."

"The Eastern District of Virginia (EDVA) is at the forefront of ensuring that American internet infrastructure is unavailable for use by international terrorist organizations, their members and affiliates," said U.S. Attorney Jessica D. Aber for the EDVA. "The domains seized through this operation are controlled by individuals and entities engaged in planning or perpetrating acts of terrorism against Americans and thus are not lawfully permitted to use American infrastructure. Operations like this disrupt terrorist activity by blocking one avenue these groups and individuals use to gather support and influence."

"This seizure demonstrates the FBI's persistence in using all of our tools to hold accountable terrorists and their affiliates when they violate U.S. laws," said Assistant Director Robert R. Wells of the FBI's Counterterrorism Division. "The FBI, along with our international partners, will continue to seek out those individuals who contribute to the advancement of Lebanese Hezbollah's malign activities and ensure they are brought to justice, regardless of where, or how, they attempt to hide."

"These court-authorized domain seizures reflect the FBI's continued dedication to the fight against terrorism," said Special Agent in Charge Keri Farley of the FBI Atlanta Field Office. "Along with our federal and international partners, the FBI remains focused on proactively disrupting web domains controlled by Specially Designated Nationals – those who attempt to illegally utilize U.S. infrastructure to incite deadly violence against the United States and our allies to further the objectives of foreign terrorist organizations."

"Today's seizure reduces Hezbollah's ability to peddle their dangerous violent ideology across the globe," said Matthew S. Axelrod, Assistant Secretary for Export Enforcement at the Department of Commerce. "This coordinated enforcement action demonstrates that the U.S. Government will creatively use all available enforcement tools to thwart those who seek to perpetrate acts of terror."

*(*Continued On The Following Column)*

Pursuant to the International Emergency Economic Powers Act (IEEPA), SDNs and SDGTs, such as Lebanese Hezbollah, Al Manar TV, Ali Damush, Ibrahim al-Sayyid, Islamic Charitable Emdad Committee, Martyrs' Foundation in Lebanon, Naim Qasim, and their members may not obtain services, including website and domain services, in the United States without a license from the Office of Foreign Assets Control (OFAC). No such license was obtained for any of the 13 seized domains.

Additionally, these 13 domains are subject to seizure as assets of entities and organizations engaged in planning or perpetrating acts of terrorism against the United States, its citizens and residents, and their property. These domains also afford a source of influence over those entities and organizations. The seizure of these domains will cut off that source of support and influence.

Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division, U.S. Attorney Jessica D. Aber for the Eastern District of Virginia, Special Agent in Charge Keri Farley of the FBI Atlanta Field Office and Assistant Secretary of Commerce for Export Enforcement Matthew S. Axelrod made the announcement.

The FBI and Department of Commerce investigated the case.

Assistant U.S. Attorneys David A. Peters and Laura D. Withers for the Eastern District of Virginia are representing the government in these matters, with valuable assistance provided by the Justice Department's National Security Division.

Attachment(s):
Download 23-sw-217 Affidavit
Topic(s):
Counterterrorism
Cybercrime
Component(s):
Federal Bureau of Investigation (FBI)
National Security Division (NSD)
USAO - Virginia, Eastern
Press Release Number:
23-538

****

READOUT: Senior Treasury and Commerce Department Officials Travel to Kazakhstan
April 27, 2023

ALMATY — From April 23 - 26, Assistant Secretary for Terrorist Financing and Financial Crimes at the U.S. Department of the Treasury Elizabeth Rosenberg and Assistant Secretary for Export Enforcement at the U.S. Department of Commerce Matthew Axelrod joined an interagency, multilateral visit to Astana and Almaty, Kazakhstan to continue close partnership on many issues, including countering the evasion of sanctions and export controls imposed on Russia for its war against Ukraine.

The delegations in Kazakhstan included Assistant Secretary Rosenberg, Assistant Secretary Axelrod, the European Union's International Special Envoy for the Implementation of EU Sanctions David O'Sullivan, and the United Kingdom's Director of the Sanctions Directorate David Reed, and were assembled to provide clarity across sanctions and export control regimes and offer technical assistance.

*(*Continued On The Following Page)*

In the face of increased efforts by Russia to illicitly procure supplies and inputs for its military-industrial complex, the delegations discussed the flows of dual-use goods of top concern and urged vigilance against an uptick in evasion attempts. They shared that in Central Asia and around the world, Russia has sought to use cut-outs, facilitate opaque payments, and exploit third countries — especially those with high levels of integration with its own economy— to circumvent sanctions and export controls.

The delegations met with government officials and the private sector to share information, outline strategic priorities, and offer assistance to help facilitate compliance while minimizing economic impacts on Kazakhstan. Assistant Secretary Axelrod shared the importance to Russia of acquiring specific semiconductors and other electronic integrated circuits to power its missiles and drones, and stressed the urgency of preventing Russia from evading coalition export restrictions by transshipping such items through Kazakhstan. Assistant Secretary Rosenberg outlined sanctions evasion typologies in the financial sector. Both noted that the United States enjoys strong partnership and open communication with the Government of Kazakhstan, and expressed the desire to be good partners to government and industry in their efforts to ensure they are not used to support the Russian war effort.

****

FOR IMMEDIATE RELEASE BUREAU OF INDUSTRY AND SECURITY -April 19, 2023 Office of Congressional and Public Affairs www.bis.doc.gov OCPA@bis.doc.gov

BIS IMPOSES $300 MILLION PENALTY AGAINST SEAGATE TECHNOLOGY LLC RELATED TO SHIPMENTS TO HUAWEI

Largest Standalone Administrative Penalty in BIS History

WASHINGTON, D.C.—Today, the Department of Commerce's Bureau of Industry and Security (BIS) imposed a $300 million civil penalty against Seagate Technology LLC of Fremont, California (Seagate US) and Seagate Singapore International Headquarters Pte. Ltd., of Singapore (Seagate Singapore) (collectively, Seagate) to resolve alleged violations of U.S. export controls related to selling hard disk drives (HDDs) to Huawei Technologies Co. Ltd. (Huawei) in violation of the foreign direct product (FDP) rule. This historic foreign direct product enforcement case and settlement represents the largest standalone administrative penalty in BIS history. Today's resolution also includes a multi-year audit requirement and a five-year suspended Denial Order.

In August 2020, BIS imposed controls over certain foreign-produced items related to Huawei, as further described below. Despite this, in September 2020, Seagate announced it would continue to do business with Huawei. Seagate did so despite the fact that its only two competitors had stopped selling HDDs to Huawei, resulting in Seagate becoming Huawei's sole source provider of HDDs. Subsequently, Seagate entered into a three-year Strategic Cooperation Agreement with Huawei, naming Seagate as "Huawei's strategic supplier" and granting the company "priority basis over other Huawei suppliers."

As alleged in the Proposed Charging Letter, BIS's investigation determined that Seagate engaged in conduct prohibited by the Export Administration Regulations (EAR) by ordering or causing the reexport, export from abroad, or transfer (in-country) of more than 7.4 million HDDs subject to the Huawei FDP rule without BIS authorization.

"The Department of Commerce is committed to robust and stringent enforcement of U.S. export controls in every corner of the world," said Deputy Secretary of Commerce Don Graves. "Today's historic action could not be possible without the deep commitment to justice and tireless work of our agents and analysts, who are contributing to the wider effort of protecting our national security." ***(*Continued On The Following Column)***

"Even after Huawei was placed on the Entity List for conduct inimical to our national security, and its competitors had stopped selling to them due to our foreign direct product rule, Seagate continued sending hard disk drives to Huawei," said Assistant Secretary for Export Enforcement Matthew S. Axelrod.

"Today's action is the consequence: the largest standalone administrative resolution in our agency's history. This settlement is a clarion call about the need for companies to comply rigorously with BIS
export rules, as our enforcement team works to ensure both our national security and a level playing field."

"Those who would violate our FDP rule restrictions are now on notice that these cases will be investigated and charged, as appropriate," said Director of the Office of Export Enforcement John Sonderman. "Any company exporting to an entity subject to the additional FDP rule restrictions needs to evaluate its entire manufacturing process to determine if specified U.S. technologies or software were used in building the essential tools used in production. Companies that discover violations should submit voluntary self-disclosures to OEE."

Additional Background on Today's Action: BIS issued an order today against Seagate imposing an administrative penalty of $300 million, mandatory multi-year audit requirement, and a five-year suspended Denial Order. As part of the BIS settlement, Seagate admitted to the conduct set forth in the Proposed Charging Letter involving Seagate US and Seagate Singapore.

BIS Case Background:
As described and alleged in greater detail in the Proposed Charging Letter (PCL), between approximately August 17, 2020, and September 29, 2021, Seagate US and Seagate Singapore, working with other Seagate entities, engaged in conduct prohibited by the EAR on 429 occasions. As alleged in the PCL, Seagate ordered or caused the reexport, export from abroad, or transfer (in-country) of approximately 7,420,496 foreign-produced HDDs, valued at approximately $1,104,732,205, to Huawei entities listed on the BIS Entity List or where such entities were a party to a transaction without authorization from BIS.

The two other companies capable of making HDDs promptly—and publicly—indicated that they had ceased sales to Huawei. Of the three, only Seagate refused to stop sales and transactions involving Huawei. BIS's $300 million monetary penalty is more than twice what BIS estimates to be the company's net profits for the alleged illegal exports to or involving Huawei.

As the transactions progressed, Seagate US repeatedly authorized extending lines of credit to Huawei totaling more than $1 billion dollars between January and September 2021 resulting in an increasing volume of HDD exports to Huawei that the entity was otherwise unable to obtain. In March 2021, Seagate and Huawei even entered into a Long-Term Agreement involving a purchase agreement of over 5 million HDDs and naming Seagate a "key strategic supplier." All the while, Seagate's competitors declined similar exports.

The BIS Order, Settlement Agreement, and Proposed Charging Letter are available online here. Additional Background on Huawei and the Foreign-Produced Direct Product Rule: On May 16, 2019, Huawei and certain of its non-U.S. affiliates were added to the Entity List, imposing
licensing requirements on exports, reexports, and transfers (in-country) of all items subject to the EAR destined to or involving the listed Huawei entities. The Entity List designation was based on a determination made by the End User Review Committee, composed of the Departments of Commerce, Defense, State, Energy and, where appropriate, the Treasury "that there is reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States."

This story, reported this weekend, began Thursday last, at the tony unit 4102 of Trump Tower III, in Sunny Isles Beach, Miami FL. The FBI raided the apartment seeking further evidence into something. The owners of the condo were identified as two Russian businessmen, partners in a shell company MIC-USA LLC..

The target of the search, Unit 4102, is owned by a shell company, MIC-USA LLC, which is controlled by Oleg Sergeyevich Patsulya and Agunda Konstantinovna Makeeva, according to state records.

U.S.-Made Technology Is Flowing to Russian Airlines, Despite Sanctions

Russian customs data shows that millions of dollars of aircraft parts made by Boeing, Airbus and others were sent to Russia last year.

By Ana Swanson and Niraj Chokshi

Ana Swanson reported from Washington, and Niraj Chokshi from New York.
May 15, 2023

Last August, Oleg Patsulya, a Russian citizen living near Miami, emailed a Russian airline that had been cut off from Western technology and materials with a tempting offer.

He could help circumvent the global sanctions imposed on Rossiya Airlines after Russia's invasion of Ukraine by shuffling the aircraft parts and electronics that it so desperately needed through a network of companies based in Florida, Turkey and Russia.

"In light of the sanctions imposed against the Russian Federation, we have been successfully solving challenges at hand," Mr. Patsulya wrote, according to a criminal complaint filed Friday with the U.S. District Court in Arizona.

Mr. Patsulya and his business partner were arrested Thursday on charges of violating U.S. export controls and international money laundering in a case that illustrates the global networks that are trying to help Russia bypass the most expansive technological controls in history.

See link: **https://www.dailykos.com/stories/2023/5/15/2169536/-Now-we-know-what-the-Feds-were-after-in-their-Miami-Trump-Tower-III-condo-raid?detail=emaildkre&pm_source=DKRE&pm_medium=email**

****

The Department of State Announces Reward Offer Against Russian Ransomware Actor
05/16/2023 11:45 AM EDT

Matthew Miller, Department Spokesperson

The impacts of ransomware attacks are significant and far-reaching, with victims suffering loss and disclosure of sensitive information and disruption of critical services. Russia is a safe haven for cybercriminals, an environment in which ransomware actors are free to conduct malicious cyber operations against the United States and our partners

Today, the State Department is announcing a reward offer, under the Transnational Organized Crime Rewards Program (TOCRP), of up to $10 million, for information leading to the arrest and/or conviction of Russian national Mikhail Pavlovich Matveev for transnational organized crime. We are taking these actions Matveev for his role in ransomware incidents targeting U.S. law enforcement, businesses, and critical infrastructure around the world.

In conjunction with this action, the Department of Justice unsealed two indictments against Matveev in the District of Columbia and the District of New Jersey. The Treasury Department also imposed financial sanctions on Matveev.

****

Bureau of Industry and Security
U.S. Department of Commerce
Office of Congressional and Public Affairs
Contact: OCPA@bis.doc.gov
May 16, 2023
BIS TAKES ACTION AGAINST COMPANIES AND INDIVIDUALS FOR ATTEMPTING TO DIVERT ELECTRONICS AND AIRCRAFT PARTS TO RUSSIA

WASHINGTON, D.C. – Today, Matthew S. Axelrod, Assistant Secretary for Export Enforcement at the U.S. Commerce Department's Bureau of Industry and Security (BIS), issued a Temporary Denial Order (TDO) suspending the export privileges of Florida company MIC P&I, LLC, Russian airline Smartavia, freight forwarder Intermodal Maldives, and Oleg Patsulya and Vasilii Besedin, two Russian nationals residing in Florida, for diverting civilian aircraft parts to Russia. The TDO is available online here: **https://efoia.bis.doc.gov/index.php/documents/export-violations/export-violations-2023/1507-e2846/file**

In a related action, the U.S. Department of Justice unsealed a four-count indictment in the District of Arizona charging Oleg Patsulya and Vasilii Besedin for conspiracy to violate the Export Control Reform Act and money laundering violations to benefit the Russian civilian aviation industry.

The coordinated enforcement actions are part of a series of actions announced today as part of the first wave of actions taken by the Disruptive Technology Strike Force, which is co-led by the Department of Commerce and the Department of Justice. The complete list of actions announced today is available here: **https://www.justice.gov/opa/pr/justice-department-announces-five-cases-part-recently-launched-disruptive-technology-strike**

"Today's coordinated actions demonstrate our resolve in impeding Russian attempts to circumvent our export controls to support their defense and civilian aircraft operations," said Assistant Secretary Axelrod. "We will aggressively use all of our criminal and administrative enforcement authorities, including the imposition of temporary denial orders, to help prevent Putin from acquiring the material he needs to prosecute his unlawful and unprovoked invasion of Ukraine."

TDOs are some of the most significant civil sanctions BIS can issue, cutting off not only the right to export items subject to the Export Administration Regulations (EAR) from the U.S. but also to receive or participate in exports from the United States or reexports of items subject to the EAR. The Assistant Secretary's order denies all of the export privileges described in part 764 of the EAR, which include (but are not limited to) applying for, obtaining, or using any license, license exception, or export control document, or engaging in or benefitting from such transactions, to prevent imminent violations of the EAR. The order was issued for a renewable 180-day period.

(*Continued On The Following Page)

As described in the TDO and alleged in the indictment, since at least September of 2022, Patsulya and Besedin collaborated with representatives of Smartavia Airlines, as well as Rossiya and Pobeda Airlines, to acquire U.S. origin aircraft parts and components in violation of U.S. export controls. Rossiya and Pobeda Airlines have been subject to TDOs since May and June of 2022, respectively. Patsulya and Besedin, through MIC P&I, LLC, attempted to deceive U.S. industry and government officials by claiming that the end user for their purchases was in Turkey rather than Russia, and then attempted to illicitly transship items through the Maldives. Patsulya specifically claimed to represent a group of companies that supplied U.S. aviation parts and electronics for various kinds of aircraft to civilian companies and affiliates of Russia's Ministry of Defense.

This investigation was conducted by the BIS Office of Export Enforcement's Phoenix Field Office and Boston Field Office jointly with the Federal Bureau of Investigation.

As referenced above, today's actions were coordinated through the Disruptive Technology Strike Force, an interagency law enforcement strike force co-led by the Departments of Justice and Commerce to target illicit actors, protect supply chains, and prevent critical technology from being acquired by authoritarian regimes and hostile nation-states. Under the leadership of the Assistant Secretary of Commerce for Export Enforcement and the Assistant Attorney General for National Security, the Strike Force leverages tools and authorities across the U.S. Government in order to enhance the criminal and administrative enforcement of export control laws.

Authorities and Export Enforcement Contact:

These BIS actions were taken under the authority of the Export Control Reform Act of 2018 and its implementing regulations, the EAR.

BIS controls exports, reexports, and in-country transfers 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. For more information, please visit: https://www.bis.doc.gov/index.php/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.

****

ChatGPT chief says artificial intelligence should be regulated by a US or global agency

The head of the artificial intelligence company that makes ChatGPT told Congress on Tuesday that government intervention will be critical to mitigating the risks of increasingly powerful AI systems.

"As this technology advances, we understand that people are anxious about how it could change the way we live. We are too," OpenAI CEO Sam Altman said at a Senate hearing.

Altman proposed the formation of a U.S. or global agency that would license the most powerful AI systems and have the authority to "take that license away and ensure compliance with safety standards."

(*Continued On The Following Column)

His San Francisco-based startup rocketed to public attention after it released ChatGPT late last year. The free chatbot tool answers questions with convincingly human-like responses.

What started out as a panic among educators about ChatGPT's use to cheat on homework assignments has expanded to broader concerns about the ability of the latest crop of "generative AI" tools to mislead people, spread falsehoods, violate copyright protections and upend some jobs.

And while there's no immediate sign Congress will craft sweeping new AI rules, as European lawmakers are doing, the societal concerns brought Altman and other tech CEOs to the White House earlier this month and have led U.S. agencies to promise to crack down on harmful AI products that break existing civil rights and consumer protection laws.

Sen. Richard Blumenthal, the Connecticut Democrat who chairs the Senate Judiciary Committee's subcommittee on privacy, technology and the law, opened the hearing with a recorded speech that sounded like the senator, but was actually a voice clone trained on Blumenthal's floor speeches and reciting ChatGPT-written opening remarks.

The result was impressive, said Blumenthal, but he added, "What if I had asked it, and what if it had provided, an endorsement of Ukraine surrendering or (Russian President) Vladimir Putin's leadership?"

The overall tone of senators' questioning was polite Tuesday, a contrast to past congressional hearings in which tech and social media executives faced tough grillings over the industry's failures to manage data privacy or counter harmful misinformation. In part, that was because both Democrats and Republicans said they were interested in seeking Altman's expertise on averting problems that haven't yet occurred.

Blumenthal said AI companies ought to be required to test their systems and disclose known risks before releasing them, and expressed particular concern about how future AI systems could destabilize the job market. Altman was largely in agreement, though had a more optimistic take on the future of work.

Pressed on his own worst fear about AI, Altman mostly avoided specifics, except to say that the industry could cause "significant harm to the world" and that "if this technology goes wrong, it can go quite wrong."

But he later proposed that a new regulatory agency should impose safeguards that would block AI models that could "self-replicate and self-exfiltrate into the wild" — hinting at futuristic concerns about advanced AI systems that could manipulate humans into ceding control.

That focus on a far-off "science fiction trope" of super-powerful AI could make it harder to take action against already existing harms that require regulators to dig deep on data transparency, discriminatory behavior and potential for trickery and disinformation, said a former Biden administration official who co-authored its plan for an AI bill of rights.

"It's the fear of these (super-powerful) systems and our lack of understanding of them that is making everyone have a collective freak-out," said Suresh Venkatasubramanian, a Brown University computer scientist who was assistant director for science and justice at the White House Office of Science and Technology Policy. "This fear, which is very unfounded, is a distraction from all the concerns we're dealing with right now."

(*Continued On The Following Page)

OpenAI has expressed those existential concerns since its inception. Co-founded by Altman in 2015 with backing from tech billionaire Elon Musk, the startup has evolved from a nonprofit research lab with a safety-focused mission into a business. Its other popular AI products include the image-maker DALL-E. Microsoft has invested billions of dollars into the startup and has integrated its technology into its own products, including its search engine Bing.

Altman is also planning to embark on a worldwide tour this month to national capitals and major cities across six continents to talk about the technology with policymakers and the public. On the eve of his Senate testimony, he dined with dozens of U.S. lawmakers, several of whom told CNBC they were impressed by his comments.

Also testifying were IBM's chief privacy and trust officer, Christina Montgomery, and Gary Marcus, a professor emeritus at New York University who was among a group of AI experts who called on OpenAI and other tech firms to pause their development of more powerful AI models for six months to give society more time to consider the risks. The letter was a response to the March release of OpenAI's latest model, GPT-4, described as more powerful than ChatGPT.

The panel's ranking Republican, Sen. Josh Hawley of Missouri, said the technology has big implications for elections, jobs and national security. He said Tuesday's hearing marked "a critical first step towards understanding what Congress should do."

A number of tech industry leaders have said they welcome some form of AI oversight but have cautioned against what they see as overly heavy-handed rules. Altman and Marcus both called for an AI-focused regulator, preferably an international one, with Altman citing the precedent of the U.N.'s nuclear agency and Marcus comparing it to the U.S. Food and Drug Administration. But IBM's Montgomery instead asked Congress to take a "precision regulation" approach.

"We think that AI should be regulated at the point of risk, essentially," Montgomery said, by establishing rules that govern the deployment of specific uses of AI rather than the technology itself.

****

Boston startup launches first commercial weather radar satellite

Tomorrow.io plans an eventual constellation of more than 20 spacecraft

Boston startup Tomorrow.io successfully launched its first weather radar satellite last month, marking a new achievement for the commercial space industry. The satellite is the first of its kind and is intended to be the start of a constellation of radar-equipped spacecraft, helping to improve forecasting of killer storms and increase the accuracy of climate models.

Prior weather satellites equipped with radar, used to see through clouds and measure precipitation, have been owned by governments or research groups.

The first-ever commercial weather radar satellite, dubbed "Pathfinder," went up on a SpaceX Falcon 9 rocket on April 14 from Vandenberg Space Force Base in California and has been responding to communications and sending back radar data for several weeks, John Springmann, vice president of space and sensors at the company, told the Globe. The washing machine-sized satellite is orbiting at an altitude of about 300 miles.

(*Continued On The Following Column)

"As novel as this is, it is working as we expected," Springmann said. "No surprises — it's going well."

Tomorrow.io, originally named ClimaCell, already provides highly detailed weather forecasts using data from ground reports for customers including JetBlue, National Grid, and the New England Patriots. It first announced the planned expansion into space two years ago.

Later this year, Tomorrow.io will launch a second, similar satellite. If the two spacecraft prove the concept works, the company plans to launch the bulk of an eventual constellation of more than 20 satellites with active radar and passive microwave gear in 2024 and early 2025. Radar allows accurate measurement of rain and snow beyond the capabilities of traditional imaging weather satellites.

Current weather radar is primarily provided by ground stations. Though the United States has a comprehensive ground network, less wealthy countries have spotty coverage and the oceans lack coverage except by a NASA satellite that provides infrequent passes. Once in operation, Tomorrow.io's constellation aims to provide radar coverage of the entire globe every hour.

The weather-tech startup abandoned plans to merge with a blank-check company last year, a deal that could have raised more than $400 million and given the company a publicly listed stock. That may have been for the best — many other companies that went public by merging with a special purpose acquisition company, or SPAC, have run into trouble. For example, Boston-based wireless Internet firm Starry Group Holdings filed for bankruptcy in February, less than a year after its SPAC merger.

Still, Tomorrow.io has continued to grow and move forward with its satellite plan without the SPAC backing. It currently employs about 200 people split between Boston, Tel Aviv, and remote locations.

The successful launch of the first satellite could help the company raise further backing, venture capitalist Ethan Batraski said. Batraski, a partner at Venrock, has invested in some space startups, but not Tomorrow.io.

"For any upstart commercial space company, launching a spacecraft successfully into orbit and operations is the single most important de-risking milestone for its future success and growth," Batraski said. The success, he added, helps convince supporters "to continue investing and funding future spacecraft."

****

COUNTRY RECEIPT OF ITAR GOODS BY CATEGORY

Foreign Countries and International Organizations for Fiscal Year 2022 as required by Section 655 of the Foreign Assistance Act of 1961, as Amended

Overview
This report documents defense articles and defense services licensed for permanent export under Section 38 of the Arms Export Control Act (AECA), 22 U.S.C. 2778, to each foreign country and international organization during fiscal year (FY) 2022, in response to the requirements in Section 655(b)(3) of the Foreign Assistance Act (FAA) of 1961, as amended. The Department of Defense will report International Military Education and Training activities separately

https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=4e3969241beaad102dc36311f54bcb16

(*Continued On The Following Column)

Report to Congress on
End-Use Monitoring of Defense Articles and Defense Services

22 USC 2785(c): End-Use Monitoring of Defense Articles and Defense Services

This report summarizes the Department of State's administration of the Blue Lantern end-use monitoring program for Fiscal Year (FY) 2022. The Blue Lantern program fulfills requirements stipulated in section 40A of the Arms Export Control Act (AECA) (22 U.S.C. 2785) and delegated to the Department of State in Executive Order 13637 (March 8, 2013).1 The program monitors the end-use of defense articles, including technical data, and defense services exported through commercial channels, as well as brokering activities, subject to Department of State licenses or other approvals under section 38 of the AECA and the International Traffic in Arms Regulations (ITAR) (22 CFR Parts
120-130), which implement section 38 of the AECA. The Blue Lantern program is managed by the Country and End-Use Analysis Division (CEA), Office of Defense Trade Controls Policy, Directorate of Defense Trade Controls (DDTC), Bureau of Political-Military Affairs.

The Blue Lantern program's mission is to help ensure the security and integrity of U.S. defense trade. The program is designed to minimize the risk of diversion and unauthorized use of U.S. defense articles, combat gray arms trafficking, uncover violations of the AECA, and build confidence and cooperation among defense trade partners.

https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=061652e31b5aa5102dc36311f54bcb00

****

Secret Service investigating intrusion at national security adviser Jake Sullivan's home
Story by Jacob Knutson • Tuesday

The Secret Service has opened an investigation into how an intruder was able to get inside White House national security adviser Jake Sullivan's home in the middle of the night a few weeks ago, a spokesperson from the agency said on Tuesday.

Why it matters: Sullivan's home was breached even though he, as a senior White House staff member, has a round-the-clock Secret Service detail assigned to him.

The intrusion, which was first reported by the Washington Post, occurred around 3 a.m. one night in late April after a man walked into Sullivan's home in the West End neighborhood of Washington D.C.

- Sullivan confronted the man and told him to leave, and agents assigned to the house were unaware of the intrusion until after the man had already left and Sullivan alerted them, according to the Post, citing three government officials.
- There were no signs of forced entry and the man appeared to be intoxicated and confused about where he was.

What they're saying: "While the protectee was unharmed, we are taking this matter seriously and have opened a comprehensive mission assurance investigation to review all facets of what occurred," Secret Service spokesperson Anthony Guglielmi said in a statement on Tuesday.

https://www.msn.com/en-us/news/politics/secret-service-investigating-intrusion-at-national-security-adviser-jake-sullivan-s-home/ar-AA1bhuLv

MISSION STATEMENT:

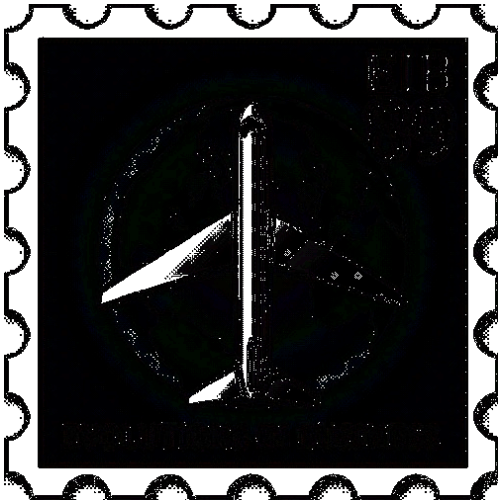
Given the geopolitical state of affairs with China, Russia, and Crimea, the Occupied territories of UKRAINE, Donetsk and Luhansk Oblast, embargoed countries and other specific threatening end users and entities, located in the United States and around the globe;

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



Stay up to date by listening to EIB's latest podcasts which you can access on our website: https://www.eib.com/EIB-Podcasts.html