EIB World Trade Headlines

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

December 15, 2020 - Volume 12, Issue 21

CELEBRATING OVER 30 YEARS

Thank You.

As 2020 winds down, we're celebrating you and all you have achieved during this unprecedented year.

Through grit, determination, and ingenuity, U.S. firms exported $2.2 trillion* U.S.-made products and services to customers around the world.

** Fiscal Year 2020. Source: U.S. Census Bureau, Economic Indicators Division*

NEWSLETTER NOTES

Taiwan Company Pleads Guilty to Trade Secret Theft in Criminal Case Involving PRC State-Owned Company

The Department of Justice today announced that United Microelectronics Corporation, Inc. (UMC), a Taiwan semiconductor foundry, pleaded guilty to criminal trade secret theft and was sentenced to pay a $60 million fine, in exchange for its agreement to cooperate with the government in the investigation and prosecution of its co-defendant, a Chinese state-owned-enterprise.

A federal grand jury had indicted UMC in September 2018, along with Fujian Jinhua Integrated Circuit Co., Ltd. (Fujian Jinhua), a state-owned enterprise of the People's Republic of China (PRC), and three individuals for conspiracy to steal, convey, and possess stolen trade secrets of an American semiconductor company (Micron Technology, Inc. (Micron)) for the benefit of a state-owned enterprise of the PRC (Fujian Jinhua). As a result of today's guilty plea, and in accordance with an accompanying plea agreement, UMC, whose American Depository Receipts are publicly traded on the New York Stock Exchange, will pay the fine—the second largest ever in a criminal trade secret prosecution, be subject to a three-year term of probation, and cooperate with the United States.

"UMC stole the trade secrets of an American leader in computer memory to enable China to achieve a strategic priority: self-sufficiency in computer memory production without spending its own time or money to earn it," said Deputy Attorney General Jeffrey A. Rosen. "This prosecution is an example of the Department of Justice's successful efforts to defend American companies from those who try to cheat and steal their technology."

UMC pleaded guilty to a superseding information charging the company with one count of criminal trade secret theft in violation of 18 U.S.C. § 1832(a)(3). The other criminal charges and a parallel civil suit by the United States against UMC will be dismissed. The criminal prosecution of Fujian Jinhua and the three individual defendants will continue, as will a civil action seeking to enjoin Fujian Jinhua from the further transfer of stolen trade secrets and the export to the United States of products manufactured by Fujian Jinhua that were made using the stolen trade secrets.

"UMC's guilty plea points this case towards trial against Fujian Jinhua in 2021," said U.S. Attorney David L. Anderson. "Criminal trade secrets cases protect freedom and innovation. These cases have global significance when a foreign defendant is charged with stealing intellectual property protected by U.S. law."

*(*Continued On The Following Column)*

"Protecting American intellectual property and trade secrets is a top priority for the FBI. This is especially true for the FBI's San Francisco Division, with Silicon Valley in our area of responsibility, and we will continue to lead the fight in safeguarding U.S. innovation from foreign adversaries," said FBI Special Agent in Charge Craig Fair. "This case sends an important message to Bay Area companies: if you report suspicious activity to the FBI, we will follow all investigative leads to identify and prosecute those responsible."

According to the facts admitted in connection with the guilty plea, UMC hired the three individual defendants—Chen Zhengkun, a.k.a. Stephen Chen; He Jianting, a.k.a. J.T. Ho; and Wang Yungming, a.k.a. Kenny Wang—from Micron's Taiwan subsidiary. UMC made Chen a senior vice president and assigned him to lead negotiation of an agreement with Fujian Jinhua to develop Dynamic Random Access Memory (DRAM) technology for Fujian Jinhua. As a foundry company, UMC previously made logic chips designed by other companies but did not make DRAM memory chips. Chen hired Ho and Wang to join the DRAM development team, and Ho and Wang brought Micron's confidential information to UMC from Micron's Taiwan subsidiary. After UMC's Information Technology Department found Micron's intellectual property on Ho's UMC computer, Chen approved the issuance of two "off network" laptop computers that allowed UMC employees to access Micron confidential information without further detection by UMC's IT department. In particular, Wang used one file containing Micron's trade secrets to adjust UMC's design rules for the memory in question. Later, when Taiwan authorities searched UMC's offices, Ho and Wang asked another UMC employee to hide papers, notes, USB drives, a personal phone, and a laptop computer while the Taiwan authorities executed their search warrants. Taiwan authorities recovered only one of the two off-network laptops. The hard drive of the other was reformatted and concealed from Taiwan authorities. Beginning in the month of the Taiwan raids, Chen became president of Fujian Jinhua and took charge of its memory production facility.

This prosecution is a result of an investigation by the FBI. Substantial assistance was provided by Taiwan's Ministry of Justice, its Ministry of Justice Investigation's Bureau (MJIB), and the Taichung District Prosecutor's Office (TDPO).

Topic(s):
Counterintelligence and Export Control
National Security
Component(s):
National Security Division (NSD)
Office of the Deputy Attorney General
USAO - California, Northern

CBP- THE TRUTH BEHIND COUNTERFEITS

The dangers of buying counterfeit products aren't always obvious. There are economic impacts, legal implications, and health and safety risks that are important for you to know before you buy. When traveling, buy from reputable sources.

Economic Impacts **-** Each year, CBP seizes all kinds of counterfeit products from all over the world. Counterfeiters look to make profits by making fake versions of the hottest products as soon they are available on the market. Each time you buy a counterfeit good, a legitimate company loses revenue. This translates to lost profits and U.S. jobs over time. Know who you buy from.

Health and Safety **-** Counterfeiters don't care about your well-being. They just want to make a profit. Many counterfeit products are low-quality and can cause injuries. Last year, CBP seized more items that pose health and safety risks than ever before. The top three categories were personal care, pharmaceuticals, and consumer electronics. Protect yourself and your family by avoiding potentially risky items.

Legal Implications - It is illegal to purchase counterfeit goods. Bringing them into the United States may result in civil or criminal penalties. Purchasing counterfeit goods supports criminal activities such as money laundering and trafficking in illegal guns and drugs. Remember, if it seems like a steal, it is.

E-Commerce - E-Commerce is a growing segment of the U.S. economy and has been increasing significantly for the past several years. Consumer habits are changing as the internet allows individuals to make purchases online. These advances in economic activity have led to increasing volumes of imports of small, just-in-time packages, creating inspection challenges for CBP. E-Commerce shipments pose the same health, safety, and economic security risks as containerized shipments, but the volume is higher and continues to grow. Additionally, transnational criminal organizations are shipping illicit goods to the United States via small packages due to a perceived lower interdiction risk and less severe consequences if the package is interdicted.

https://www.cbp.gov/FakeGoodsRealDangers

Former Raytheon Engineer Sentenced for Exporting Sensitive Military-Related Technology to China

FOR IMMEDIATE RELEASE
Tuesday, November 17, 2020

TUCSON, Ariz. – Today, Wei Sun, 49, a Chinese national and naturalized citizen of the United States, was sentenced to 38 months in prison by District Court Judge Rosemary Marquez. Sun previously pleaded guilty to one felony count of violating the Arms Export Control Act (AECA).

Sun was employed in Tucson for 10 years as an electrical engineer with Raytheon Missiles and Defense. Raytheon Missiles and Defense develops and produces missile systems for use by the United States military. During his employment with the company, Sun had access to information directly related to sensitive defense technology. Some of this defense technical information constituted what is defined as "defense articles," which are controlled and prohibited from export without a license under the AECA and the International Traffic in Arms Regulations (the ITAR).

From December 2018 to January 2019, Sun traveled from the United States to China on a personal trip. On that trip, Sun brought along unclassified defense-related technical information in his company-issued computer, including data associated with an advanced missile guidance system that was controlled and regulated under the AECA and the ITAR. Despite having been trained to handle these materials correctly, Sun knowingly transported the information to China without an export license in violation of the AECA and the ITAR.

"Sun was a highly skilled engineer entrusted with sensitive missile technology that he knew he could not legally transfer to hostile hands," said Assistant Attorney General John C. Demers. "Nevertheless, he delivered that controlled technology to China. Today's sentence should stand as a warning to others who might be tempted similarly to put the nation's security at risk."

"The United States relies on private contractors to help build our unparalleled defense technology," said United States Attorney Michael Bailey. "People who try to expose that technology to hostile foreign powers should know that prison awaits them. The close cooperation of the victim defense contractor and the dedication of the FBI made this case a success."

*(*Continued On The Following Page)*

"Sun admitted to illegally exporting controlled weapons technology plans out of the U.S. to China." said Sean Kaul Special Agent in Charge of the FBI Phoenix Field Office. "China represents the greatest counterintelligence threat to our nation's protected information and intellectual property. Confronting this threat remains a top priority for the FBI and we applaud the victim company for their cooperation and coordination throughout this investigation. We encourage Americans to be aware of the foreign economic espionage threat and report any relevant information to their local FBI office." The Federal Bureau of Investigation, investigated this matter with the assistance of Raytheon Missile and Defense. Beverly K. Anderson and Nicole P. Savel, Assistant United States Attorneys, and William Mackie from the National Security Division, Counterintelligence and Export Control Section, handled the prosecution.

L3Harris Technologies to Invest $1.5M in Rhode Island for Navy Sonar Work

L3Harris Technologies will expand in Rhode Island as part of recent growth in its towed array sonar work for the U.S. Navy. Shown here is the company's Model 980 Active Low Frequency Towed Sonar (ALOFTS). L3Harris Technologies
ASHAWAY, R.I. — L3Harris Technologies, an aerospace and defense technology company, plans to expand in Ashaway, Rhode Island, by investing $1.5 million in its operations, the company said in a Nov. 24 release. The company will add more than 40 positions and increase its manufacturing space to 92,000 square feet.

The L3Harris facility develops and manufactures technology the U.S. Navy uses in submarines for surveillance and detection. The expansion will support the Navy's recent contract award of $31 million for L3Harris to build next-generation towed sonar systems for submarines. The facility expansion will be equipped with state-of-the-art sonar array manufacturing and environmental test equipment to enhance the product's overall performance.

"The Ashaway facility expansion represents a long-standing commitment to meeting the Navy's current and future needs and creating job opportunities in Rhode Island," said Scott Tilden, vice president and general manager, Maritime Sensors, L3Harris. "This facility has an exceptional record of designing, developing, and manufacturing undersea sensors, which is one of the exciting reasons we continue to invest and expand operations in the state."
L3Harris' Ashaway location has provided undersea sensor systems since 1991, including the TB-29C and TB-34A towed array sonars. Other support to the Navy includes providing integrated solutions for ship monitoring, ship defense sensors, submarine electronics and acoustic sensors for unmanned vehicles.

DOD initiative advocates industrial workforce

Wednesday, November 25, 2020 by Douglas Clark

The Department of Defense (DOD) has awarded its first nine prototyping projects to bolster the industrial workforce sector. The projects, valued at nearly $27 million, are in conjunction with the National Imperative for Industrial Skills initiative, also known as the Skills Imperative.

" A skilled workforce has been the bedrock of our economic security and when needed our national security," Jeffrey "Jeb" Nadaner, deputy assistant secretary of defense for industrial policy, said. "The next arsenal of democracy will be built by American hands and creative minds. Thousands of manufacturing jobs in our defense industrial base await Americans seeking careers with purpose and fulfillment. Whether building automobiles, aircraft carriers or nuclear submarines, the Skills Imperative invites industry allies to rally alongside the department and help Americans develop the necessary skills to be part of these production efforts."

The DOD's industrial policy office previously issued a standing, five-year request to academia and industry for innovative prototyping proposals addressing selected key segments of the industrial skills workforce development ecosystem, officials said, noting the initial awards have been earmarked for endeavors in Texas, Alabama, Missouri, Tennessee, Virginia, Illinois, Connecticut, Rhode Island, and New Hampshire.

Adele Ratcliff, Industrial Base Analysis and Sustainment program office director, said she is confident the effort would enable greater stakeholder cooperation across the industrial base and encourage more partners to come forward to join the effort to drive sufficient scale and velocity into industrial workforce development pipelines

Notice of Request for Public Comments on Condition of the Public Health Industrial Base and Recommend Policies and Actions To Strengthen the Public Health Industrial Base To Ensure Essential Medicines, Medical Countermeasures, and Critical Inputs Are Made in the United States.

12/2/20

85 FR 77428

Notice of Request for Public Comments on Condition of the Public Health Industrial Base and Recommend Policies and Actions To Strengthen the Public Health Industrial Base To Ensure Essential Medicines, Medical Countermeasures, and Critical Inputs Are Made in the United States.

On August 6, 2020, President Trump issued an Executive order, Combating Public Health Emergenciesand Strengthening National Security by Ensuring Essential Medicines, Medical Countermeasures, and Critical Inputs Are Made in the United States. Among other directives, the E.O. directed that, by February 2, 2021, the Secretary of Commerce shall submit a report to the Director of the Office of Management and Budget, the Assistant to the President for National Security Affairs,

the Director of the National Economic Council, and the Director of the Office of Trade and Manufacturing Policy, describing any change in the status of

the Public Health Industrial Base (PHIB) and recommending initiatives to strengthen the PHIB. This notice requests comments from the public to assist the Department of Commerce (referred to henceforth as ''Commerce'') in preparing this report on the condition of the PHIB and recommending policies and actions to strengthen the PHIB.

Due date for filing comments is 12/23/20.

Commerce Department Terminates Section 232 Investigation into Mobile Crane Imports

FOR IMMEDIATE RELEASE
BUREAU OF INDUSTRY AND SECURITY
December 04, 2020
Office of Congressional and Public Affairs
www.bis.doc.gov
(202) 482-1069

Commerce Department Terminates Section 232 Investigation into Mobile Crane Imports

WASHINGTON…On November 23, 2020, Secretary Ross terminated an investigation, which was initiated under Section 232 of the Trade Expansion Act, into whether imports of mobile cranes threaten to impair U.S. national security. The investigation was terminated following a September 8, 2020 request from the applicant, The Manitowoc Company, Inc., to withdraw its application and terminate the investigation, citing a changing economic environment due to the effects of the COVID-19 pandemic.

The Secretary initiated the investigation in May that included a public comment period. After consideration of Manitowoc's request for withdrawal, the Secretary determined that it was appropriate to terminate the investigation. The Department of Commerce will publish a *Federal Register* notice informing the public of this decision.

FireEye hack: Cybersecurity firm says nation-state stole attacking tools

"This attack is different from the tens of thousands of incidents we have responded to throughout the years," the firm says in an SEC filing.
Major cybersecurity firm FireEye has been hit by a cyberattack, with hackers stealing its attack test tools in a targeted heist, the company said in a blog post Tuesday. CEO Kevin Mandia said the hack most likely came from a nation-state attacker.

The hack hit one of the largest cybersecurity companies in the US. FireEye has investigated prominent cyberattacks including the Equifax breach and the Democratic National Committee hack. The hackers stole FireEye's "Red Team" tools, a collection of malware and exploits used to test customers' vulnerabilities. Mandia said none of the tools was a zero-day exploit (a vulnerability that doesn't have a fix).

*(*Continued On The Following Page)*

"Based on my 25 years in cyber security and responding to incidents, I've concluded we are witnessing an attack by a nation with top-tier offensive capabilities," Mandia said in his post. "This attack is different from the tens of thousands of incidents we have responded to throughout the years. The attackers tailored their world-class capabilities specifically to target and attack FireEye."

The firm said it's working with the FBI to determine how it was hacked, as well as with partners like Microsoft.

"The FBI is investigating the incident, and preliminary indications show an actor with a high level of sophistication consistent with a nation-state," said the FBI Cyber Division's assistant director, Matt Gorham. Microsoft confirmed that it's assisting with the investigation and noted that the hackers used a rare combination of techniques to steal FireEye's tools.

"This incident demonstrates why the security industry must work together to defend against and respond to threats posed by well-funded adversaries using novel and sophisticated attack techniques," Microsoft said in a statement. "We commend FireEye for their disclosure and collaboration, so that we can all be better prepared."

Mandia said FireEye hasn't seen any evidence that its stolen tools have been used, but the company will continue to monitor for any activity. FireEye has also released countermeasures for its own attacking toolson GitHub. In a Securities and Exchange Commission filing, FireEye noted that the attacker's methods were highly sophisticated, using techniques that would cover tracks and make any forensics investigations difficult. The combination of techniques hadn't been seen before by the company, Mandia said.

Cybersecurity companies aren't immune to hacks just because it's their job to defend against them. Firms like Symantec, Kaspersky and Trend Micro have all suffered attacks in the past.

In 2017, a group of hackers stole cyberattack tools from the US National Security Agency, which allowed for rampant hacks like the WannaCry ransomware campaign.

FireEye said it hasn't seen any evidence that the hackers stole data from the company or took any information about its customers.

"This news about FireEye is especially concerning because reportedly a nation-state actor made off with advanced tools that could help them mount future attacks," Rep. Adam Schiff, chairman of the House Select committee on Intelligence, said. "We have asked the relevant intelligence agencies to brief the committee in the coming days about this attack, any vulnerabilities that may arise from it, and actions to mitigate the impacts."

*(*Continued On The Following Column)*

Sen. Mark Warner, a Democrat from Virginia and co-chair of the Senate Cybersecurity Caucus, commended FireEye for disclosing the attack, and urged other potential victims to do the same.

"We have come to expect and demand that companies take real steps to secure their systems, but this case also shows the difficulty of stopping determined nation-state hackers," Warner said. "As we have with critical infrastructure, we have to rethink the kind of cyber assistance the government provides to American companies in key sectors on which we all rely."

First published on Dec. 8, 2020 at 1:40 p.m. PT.

U.S. Secretary of Commerce Wilbur Ross and Singapore Minister for Trade and Industry Chan Chun Sing Sign Memorandum of Understanding on Trade Financing and Investment Cooperation

FOR IMMEDIATE RELEASE
Tuesday, December 15, 2020

News Media Contact:
Office of Public Affairs, 202-482-4883

WASHINGTON – The United States of America (U.S.) and Singapore have signed a Memorandum of Understanding (MOU) to deepen economic cooperation and extend trade financing and investment support to companies in Singapore and the U.S. The MOU was signed by U.S. Secretary of Commerce Wilbur Ross and Singapore Minister for Trade and Industry Chan Chun Sing.

“The U.S. and Singapore have enjoyed more than fifty years of official partnership since we established diplomatic ties in 1966,” said Secretary Ross. “This MOU will help Singapore importers finance the purchase of U.S. exports and support Singapore investors looking at opportunities in the U.S.”

Singapore’s Minister for Trade and Industry Chan Chun Sing said, “As like-minded partners, Singapore and the U.S. are committed to supporting our businesses as they respond to the global economic disruptions caused by COVID-19.

(*Continued On The Following Page)

Through this MOU, we will facilitate company investments into Singapore and the U.S., and help businesses access more trade financing facilities. We also look forward to catalysing greater trade and investment flows between the U.S., Singapore, and Southeast Asia, and enabling our companies to continue trading and accessing opportunities in these challenging times."

The U.S. and Singapore are like-minded and longstanding partners with a strong record of economic cooperation. Recognising the significant global tightening of credit following the economic slowdown caused by the COVID-19 pandemic, the MOU aims to enhance the availability of and access to trade financing options for U.S. and Singapore companies. The MOU will also facilitate bilateral trade in goods and services to enhance our respective regions' growth opportunities. In addition, the MOU seeks to strengthen cooperation on investment promotion and provide opportunities for both countries to explore the use of technology (e.g. FinTech) to address new trade financing and investment challenges.

The renewable, two-year MOU will be overseen by the U.S. Department of Commerce and Singapore's Ministry of Trade and Industry. The MOU will also be supported by implementing agencies, including the Export-Import Bank of the U.S., the U.S. Commercial Service in Singapore, and Enterprise Singapore.

The MOU is the latest tangible result of the robust economic and investment partnership between the U.S. and Singapore. The U.S. is Singapore's largest foreign investor, while Singapore was the
fourth-largest Asian investor in the U.S. in 2019. Both countries are committed to working together towards a stronger post-COVID-19 economic recovery. Our continued partnership will help to facilitate bilateral trade and investments and ensure that our companies are well positioned to tap into growth opportunities in our respective markets and regions.

FOR IMMEDIATE RELEASE BUREAU OF INDUSTRY AND SECURITY

FOR IMMEDIATE RELEASE BUREAU OF INDUSTRY AND SECURITY December 14, 2020
Office of Congressional and Public Affairs www.bis.doc.gov
(202) 705-9067

Commerce Imposes License Restrictions after Turkey's Acquisition of Russian Missiles Statement from a BIS spokesperson: The Bureau of Industry and Security (BIS) in the Department of Commerce implemented a policy of denial for export license applications to the Turkish Presidency of Defense Industries (SSB) as a result of its acquisition of the S-400 long-range surface-to-air missile system from Russia. BIS coordinated this action with the Department of State, which imposed sanctions on the SSB pursuant to the Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA) as a result of the missile deal.

Addition of 'Military End User' (MEU) List to the Export Administration Regulations and Addition of Entities to the MEU List

12/23/2020

85 FR 83793

In this final rule, the Bureau of Industry and Security (BIS) amends the Export Administration Regulations (EAR) by adding a new 'Military End User' (MEU) List that includes the first tranche of entities. The U.S. Government has determined that these entities are 'military end users' for purposes of the 'military end user' control in the EAR that applies to specified items for exports, reexports, or transfers (in-country) to the People's Republic of China (China), Russia, and Venezuela when such items are destined for a 'military end user.' The existing 'military end-use' and 'military end user' controls under the EAR, including BIS's authority to inform the public of a license requirement for an item due to an unacceptable risk of diversion to a 'military end user' via amendment to the EAR, are essential for protecting U.S. national security interests. The addition of the new MEU List via amendment to the EAR and this first tranche of entities is also responsive to requests received from the public. This final rule will add one hundred and three 'military end users' to the MEU List consisting of fifty-eight under China and forty-five under Russia. However, the establishment of the MEU List does not imply that other parties, not included on the list, are not subject to the 'military end-use' and 'military end user' controls under the EAR.

Remarks by Commerce Secretary Wilbur Ross at the Export-Import Bank Virtual Board Meeting on Domestic Content Policy

Thursday, December 17, 2020

Wilbur Ross, Secretary of Commerce

Secretary Ross: Thank you, Chairman Reed and Directors Bachus and Pryor, for your leadership of this Board, and for your work developing the proposal we are considering today, permitting EXIM to provide full financing packages for exports in designated transformational sectors containing at least 51 percent U.S. content. This change is an update over the current policy which stipulates an 85 percent requirement. Over the past 40 years, this policy has helped ensure that EXIM Bank financing supports American exports and jobs. But as the world changes and global supply chains become more complex, our competitors have adopted more flexible approaches. Germany, for instance, requires 51 percent domestic content but can approve exceptions; the United Kingdom requires only 20 percent; and Canada requires zero percent provided that the transaction benefits Canada. Furthermore, EXIM Bank's 2019 Report to the U.S. Congress on Global Export Credit Competition details how China provided $33.5 billion in financing during 2019, more than three times Italy at $11.1 billion. So I welcome the EXIM Board's consideration of this proposal today to modernize the existing U.S. content policy. The new measure aims to bolster U.S. export competitiveness, to the benefit of American exporters, jobs, and economic and national security. I understand too that if projects are deemed critical to national security in combatting China, this new proposal allows for a transaction with less than 51 percent U.S. content to also be considered for financial support from EXIM. This is critically important to U.S. exporters and foreign buyers experiencing difficulties due to the COVID-19 pandemic. And as a result, EXIM will be able to support many of the more than $1 billion in financing requests in its pipeline under the Program on China and Transformational Exports, including several water treatment and 5G telecommunications programs, among others. I am also especially pleased that this proposal includes the provision recommended by the Commerce Department requiring each applicant to submit a written action plan for expanding its U.S.-based jobs in the coming 3-5 years. This includes potentially shifting supply chains and sourcing to the United States from offshore. We must do all we can to keep our exporters viable and competitive during this time.
And my Department stands ready and willing to continue our work with EXIM as you implement your Program on China and Transformational Exports. Thank you, and I look forward to our discussion.

News Media Contact:
Office of Public Affairs, 202-482-4883

Remarks by Commerce Secretary Wilbur Ross at the Eighth Meeting of the National Space Council

AS PREPARED FOR DELIVERY
Wednesday, December 9, 2020

Wilbur Ross, Secretary of Commerce

Introduced by Vice President Mike Pence.

Secretary Ross: Thank you, Vice President Pence, for the opportunity to update the National Space Council on the growth of the space economy and the related work that is taking place at the Department of Commerce.

Here at Cape Canaveral last week, SpaceX executed its 100th successful commercial Falcon 9 rocket launch, sending a crew and thousands of pounds of supplies and research gear aboard a Dragon spacecraft to the International Space Station. I am reminded of a time not long ago when travel among the stars was merely a distant goal, before it was even a race among nations.

Indeed, our country has achieved remarkable progress in the space sector, and now again as American business people continue creating new ways to make space more commercially accessible. I toured such an example earlier this year, when I visited Astrobotic's new headquarters in Pittsburgh. Their facility will support unmanned missions to the moon and drive technological development that brings us closer to NASA's planned 2024 human moon landing.

Such landmark accomplishments in the commercial space field come alongside record-breaking economic investment in space activities. Globally, another $4.9 billion was invested in space companies in Q3 alone. This not only marks the most productive quarter on record, but it also raises total 2020 investment to $17.5 billion in the overall industry. And the United States accounts for 62 percent of the industry's cumulative investment. Morgan Stanley projects that the revenue generated by the global space industry may top $1 trillion by 2040.

The recent explosion in the industry here in the United States is owed in no small part to the efforts of the Trump Administration. The Administration's pro-space agenda and the work of the National Space Council has already had significant impacts. NOAA has been able to remove red tape that previously surrounded remote sensing technology by shortening licensing timelines from 74 days to 28 days. This enables companies to sell data from satellites more easily and efficiently, helping commercial satellite operators stay competitive in a rapidly changing global marketplace.

(*Continued On The Following Page)

The Commerce Department has also taken steps over the last year, at the behest of the Vice President, to identify new space missions and get them the necessary authorization to proceed. The goal here is to alleviate the administrative and regulatory burden on emerging companies and technologies, and we enthusiastically continue on in that mission.

Financial indicators and regulatory procedures aside, one simple way to observe the growth of our space industry is to look at the sheer number of satellites in orbit. This year alone, the number of active satellites in orbit is set to increase by more than 50 percent. The Satellite Industry Association estimates that up to 110,000 new satellites could be in orbit by 2030.

This is good news for projects like SpaceX's Starlink as well as for smaller companies that can benefit from the growing accessibility of private satellites. But the increase in satellites has also created a unique set of challenges when it comes to managing orbital traffic. We are seeing more and more frequent near misses that could create unprecedented new debris. If two significant objects were to collide, they could create a shower of debris that may endanger the astronauts aboard the International Space Station, billions of U.S and allied investment in space, and the growth of space commerce.

Fortunately, there is no shortage of brilliant men and women who have made remarkable headway toward managing this problem. In 2018, the Trump Administration's Space Policy Directive-3 provided a unique approach to the management of space traffic. The Commerce Department's Office of Space Commerce and our interagency partners took on the mission laid forth by this initiative. Today, I'm proud to report that we're in the midst of finalizing a DOC-DOD MOU that will provide a detailed plan for the improvement of space situational awareness, and ultimately, space traffic management.

We have also drawn on existing NOAA resources to establish a new open architecture data repository. This system allows both private and government entities, including those of our allies, to share data, increasing all parties' situational awareness amidst an increasingly crowded orbital environment. We continue to work with our allies and industry on the norms, standards and best practices that will inform new "rules of the road" in space.

We have also worked with private business and technology leaders from around the nation on this issue. In fact, just before Thanksgiving, the Office of Space Commerce hosted an industry day with over 250 companies participating to discuss our approach to the Open Architecture Data Repository. We will continue to work collaboratively with the public and private sector to tackle this challenge.

(*Continued On The Following Column)

It is not the only one we face. China's lunar landing last week underscores that we are not the only ones invested in the business of space, and that competition for American companies operating in this sector face real competition. Looking ahead, my Department's Bureau of Economic Analysis is set to publish innovative experimental statistics within the next two weeks that will help us further measure and understand the space sector.

I look forward to sharing this informative new data with you. The United States remains an incubator for greatness like no other, and I'm confident that we will retain our position as the premier hub for space-based exploration and business.

Thank you.

###

News Media Contact:
Office of Public Affairs, 202-482-4883

Remarks as Prepared for Delivery

Attorney General William P. Barr Delivers Remarks at the Pan Am 103 Press Conference

Washington, DC

~

Monday, December 21, 2020

On this day 32 years ago, December 21, 1988, at 7:03 p.m. local time, a bomb destroyed Pan Am Flight 103 as it flew 31,000 feet above Lockerbie, Scotland. The massive Boeing 747 plane, known as the "Clipper Maid of the Seas," exploded and fell to the ground in countless pieces scattered across 840 square miles, nearly the entire width of Scotland. The explosion killed all 259 people on board—243 passengers and 16 crew members, including 190 Americans. Falling debris claimed the lives of 11 Lockerbie residents on the ground, many of whom were in their homes and had just sat down for dinner. The Lockerbie bombing remains the deadliest single terrorist attack in the history of the United Kingdom, and the second deadliest terrorist attack for Americans—surpassed only by the 9/11 attacks.

Immediately after the bombing, the FBI partnered with law enforcement agencies from Scotland to investigate. That joint investigation led to the filing of charges in 1991 against two Libyan intelligence officers. The investigation also pointed to another conspirator—a man known by the name "Abu Agela Masud"—but at the time, investigators were unable to identify or locate that suspect.

*(*Continued On The Following Page)*

Joined this morning by Assistant Attorney General for National Security John Demers … Acting United States Attorney for the District of Columbia Michael Sherwin … and Kara Weipz, whose brother Rick Monetti was killed on the flight and who now leads a Pan Am Flight 103 advocacy organization, I am pleased to announce that the United States has filed criminal charges against the third conspirator, Abu Agila Muhammad Mas'ud Kheir Al-Marimi, for his role in the bombing of Pan Am Flight 103.

Let there be no mistake: no amount of time or distance will stop the United States, and its partners in Scotland, from pursuing justice in this case.

Well over a third of Americans alive today were not yet born on the day of the Lockerbie bombing or would not have been old enough to remember it. But for those of us who do remember, that tragic event and the iconic images of its aftermath, some of which are displayed here today, are forever seared in our memories.

Passengers and crew aboard the flight came from 21 countries around the world. But by far the largest contingent on that doomed flight were Americans, including a group of 35 study-abroad students from Syracuse University who were on their way home to spend the holidays with their families. There is no question that the Pan Am 103 attack was aimed at the United States, and this heinous assault lives in infamy in the collective memory of the American people. At Arlington National Cemetery, a cairn of 270 Scottish stones honors "those who lost their lives in this attack against America." And at Syracuse University, 35 Remembrance Scholarships are awarded each year, with each recipient representing a particular Syracuse student killed aboard the plane.

Following the bombing, many of the victims' families made an agonizing journey to Scotland to the place where they lost their loved ones. The people of Lockerbie, though devastated themselves, provided around-the-clock hospitality. In an unforgettable gesture, a group of Scottish women meticulously collected clothing from amid the wreckage; washed, ironed, and folded the garments they found; and sent them home to the victims' family members as a final connection to their loved ones. Sadly, the remains of 17 victims were never identified or found.

From the beginning, the United States and Scotland have been determined to find and hold accountable those who perpetrated the Pan Am 103 attack. As I mentioned, our joint investigation led to the filing of charges in November 1991 in both the United States and Scotland against two Libyan intelligence officers—Abdel Baset Ali al-Megrahi and Lamen Khalifa Fhimah. Nearly ten years later, in May 2000, a specially established Scottish court convened in The Netherlands to try the two men. In January 2001, Megrahi was convicted on all charges, but Fhimah was acquitted.

*(*Continued On The Following Column)*

The breakthrough that has led to the charges announced today arose when law enforcement learned in 2016 that the third conspirator had been arrested after the collapse of the Qaddafi regime and interviewed by a Libyan law enforcement officer in September 2012. According to the criminal complaint affidavit, Masud built the bomb that destroyed Pan Am Flight 103 and worked with Megrahi and Fhimah to carry out the plot. The affidavit also alleges that the operation had been ordered by the leadership of Libyan intelligence and that, after the downing of the aircraft, Qaddafi had thanked Masud for the successful attack on the United States. In addition to his involvement in the Lockerbie bombing, Masud was also involved in the 1986 bombing of the LaBelle Discotheque in Berlin, West Germany, which killed two American service members and a Turkish woman. Although Masud remains in Libyan custody, Libyan authorities provided a copy of the interview to law enforcement. Based on that and other evidence, prosecutors from the U.S. Attorney's Office for the District of Columbia and the Counterterrorism Section of the National Security Division unsealed a complaint this morning in the U.S. District Court for the District of Columbia charging Masud with terrorism-related crimes for his role in the bombing of Pan Am Flight 103. At long last, this man responsible for killing Americans and many others will be subject to justice for his crimes.

The Lockerbie bombing case holds special significance for me because I was serving as the Acting Attorney General when charges were filed against Megrahi and Fhimah in 1991. I know firsthand the toil, tears, and sweat that have been poured into pursuing justice for the victims of the Lockerbie bombing and their families. And so it is with profound gratitude that I recognize and thank our law enforcement friends in Scotland for their nearly 32-year partnership with us on this case. I also thank Lord Advocate of Scotland James Wolffe for his continued partnership. There is much work still to be done, and we will not be able to do it without our colleagues in Scotland. We are committed to working arm-in-arm with them as we move forward in this case. I am especially proud of the countless agents and analysts of the FBI who have worked the Pan Am 103 case relentlessly over the decades. Thank you for your dedication and perseverance. And finally, I thank the prosecutors in the U.S. Attorney's Office for the District of Columbia and the National Security Division for their many years of hard work and for preparing the charges in this case. Today, Masud remains in Libyan custody, and we intend to work closely with our Scottish counterparts to use every feasible and appropriate means to ensure that he answers for his part in the Lockerbie bombing. It is my hope that Libyan authorities will allow Masud to be tried for this crime and will provide the support and witnesses necessary to bring him to justice. Nevertheless, while we will never rest in our efforts to hold Masud accountable, I hope that the families of the lost will find some comfort in the charges filed today. The alleged facts underlying these charges fill important gaps in the historical record and help complete the account of how the bombing was executed and who was responsible. Finding the truth is the first step toward achieving justice.

International Trio Indicted in Austin for Illegal Exports to Russia

A four–count federal grand jury indictment returned in Austin and unsealed today charges three foreign nationals – a Russian citizen and two Bulgarian citizens – with violating the International Emergency Economic Powers Act (IEEPA), Export Control Reform Act (ECRA), and a money laundering statute in a scheme to procure sensitive radiation-hardened circuits from the U.S. and ship those components to Russia through Bulgaria without required licenses. "Time and again, we find the Russians attempting to get access to sensitive American technology. The defendants here are charged with exporting radiation-hardened chips to Russia, knowing that it was illegal to do so and establishing a business in Bulgaria to circumvent U.S. enforcement authorities," said Assistant Attorney General for National Security John C. Demers. "I am gratified by our whole-of-government response to this flagrant example of U.S. export controls evasion."

"Today's indictment demonstrates that the United States Attorney's Office, the Department of Justice and our federal partners will follow those who seek to evade U.S. export enforcement laws wherever our investigations lead. National security remains our highest priority. We must never allow our most sensitive technology to fall into the hands of those who would seek to use it against us," said U.S. Attorney Sofer.

"The Office of Export Enforcement in partnership with the FBI and DCIS uncovered an illicit procurement network that was diverting radiation-hardened integrated circuits from the United States through a Bulgarian front company to entities in Russia," said P. Lee Smith, Performing the Non-exclusive Functions and Duties of the Assistant Secretary for Export Enforcement at the Department of Commerce. "Today's announcement and related action by the Commerce Department to place the parties on the Entity List represent a collaborative whole-of-government approach to protecting sensitive, controlled U.S. technology, which is critical to our national security." "Today's indictment details the efforts our adversaries will make to obtain our sensitive technology and demonstrates that the United States will hold any individuals, organizations, and nations, who willfully violate our export laws accountable." said Special Agent in Charge Christopher Combs. "The FBI and our partners will work vigorously to protect and defend the national security of our country."

The indictment alleges that 48-year-old Russian national Ilias Sabirov, 70-year-old Bulgarian national Dimitar Dimitrov and 46-year-old Bulgarian national Milan Dimitrov used Bulgarian company Multi Technology Integration Group EEOD (MTIG) to receive controlled items from the U.S. and send them to Russia. Under U.S. export control law, the goods could not be shipped to Russia without the permission of the U.S. government.

*(*Continued On The Following Column)*

In 2014, the defendants met with the supplier of the radiation-hardened components in Austin and were informed that radiation-hardened circuits could not be shipped to Russia because of U.S. trade restrictions. Stymied by U.S. law, Sabirov established MTIG in Bulgaria and bought the controlled electronic circuits. The radiation-hardened properties of these circuits made them resistant to damage or malfunction in the harsh outer-space environment. Export of the parts was controlled by the U.S. government for these very reasons. The parts were shipped to Bulgaria in 2015 and MTIG soon thereafter shipped them to Sabirov's companies in Russia. OOO Sovtest Comp. transferred over $1 million to MTIG for controlled U.S. parts. In the same timeframe, MTIG—at Sabirov's direction—ordered over $1.7 million in other electronic components produced by another U.S. electronics manufacturer. Sabirov bought these parts to fulfill part of his contract with OOO Sovtest Comp. Again, the parts were shipped from the U.S. to Bulgaria where they were merely repackaged and onward shipped to Russia.

In late 2018, a Department of Commerce Export Control Officer interviewed Milan Dimitrov during a visit at MTIG to determine whether the radiation-hardened components were still in MTIG's possession in Bulgaria. Milan Dimitrov, among other things, fraudulently denied sending the components to Russia. The indictment charges Sabirov, Dimitar Dimitrov and Milan Dimitrov with two counts related to violations of IEEPA and one count of money laundering. The indictment also charges Milan Dimitrov with one count of false statements to the government. Each count charged in the indictment calls for up to 20 years in federal prison upon conviction.

In conjunction with the unsealing of these charges, the Department of Commerce is designating Ilias Sabirov, Dimitar Dimitrov, Milan Dimitrov, Mariana Marinova Gargova, MTIG EOOD, Cosmos Complect and OOO Sovtest Comp., adding them to its Bureau of Industry and Security Entity List. Designation on the Entity List imposes a license requirement before any commodities can be exported from the U.S. to these persons or companies and establishes a presumption that no such license will be granted. The Entity List identifies foreign parties that are prohibited from receiving some or all items subject to the Export Administration Regulations (EAR) unless the exporter secures a license. Those persons present a greater risk of diversion to weapons of mass destruction (WMD) programs, terrorism or other activities contrary to U.S. national security or foreign policy interests. Commerce – Office of Export Enforcement can add to the Entity List a foreign party, such as an individual, business, research institution or government organization, for engaging in activities contrary to U.S. national security and/or foreign policy interests. In most instances, license exceptions are unavailable for the export, re-export or transfer (in-country) to a party on the Entity List of items subject to the EAR. Rather, a prior license is required, usually subject to a policy of denial. In all cases, defendants are presumed innocent until and unless proven guilty. The indictment merely contains allegations of criminal activity.

COMMENTARY

What new CMMC rule and deadline mean to you

By Edward Tuorinsky, Derek Kernus

Oct 23, 2020

Grab a red pen and circle Nov. 30, 2020 on the calendar. That's the next deadline in the government's initiative to improve cybersecurity and every contractor has reason to mark the date. Government contractors with a DFARS 252.204-7012 clause in their contracts are required to conduct a self-assessment of NIST SP 800-171 standards and enter their results into the Supplier Performance Risk System by the end of next month.

What's the big deal, you ask?

Government contractors have long been asked to follow these standards, however, this deadline, shines a spotlight on how compliant companies really are across 110 controls, giving each company a score for their efforts. Those who don't have their results entered will not be eligible for an award on a contract containing the clause. Every control is worth 1 point, while those controls NOT met subtract up to 5 points. It's not only possible, but likely, that many companies will have to report a negative score, despite having basic cyber security protections in place. That's not a good look for a contractor or sub looking to renew or secure contract wins. The late-September DFARS announcement came as a bit of a surprise to the industry. Cybersecurity self-reporting has been a scout's honor policy with little oversight or validation until recently. The Cybersecurity Maturity Model Certification, or CMMC, a third-party certification, was already big news and rumored to start in 2021. Large contractors with teams of cyber pros on staff may be ready to demonstrate how they meet the required practices for each Maturity Level. However, small and medium sized businesses are struggling to prove their practices meet the mark—wondering if the IT investments necessary to establish higher Maturity Levels will pay off.

The connection between NIST SP 800-171 and CMMC

"Ever job is a self-portrait of the person who does it. Autograph your work with excellence."

David Wichner

A former engineer at Tucson-based Raytheon Missiles & Defense was sentenced to more than three years in federal prison for violating federal arms-control laws by taking a company laptop computer to China.Wei Sun, 49, a Chinese national and naturalized U.S. citizen, was sentenced to 38 months in prison Tuesday by U.S. District Judge Rosemary Marquez.Sun had pleaded guilty to one felony count of violating the Arms Export Control Act for taking a Raytheon laptop containing unclassified defense data on a trip to China from December 2018 to January 2019.Sun was employed in Tucson for 10 years as an electrical engineer and had access to information directly related to sensitive missile technology, the U.S. Attorney's Office said.Some of the defense technical information Sun had is defined as "defense articles," which are controlled and prohibited from export without a license under the AECA and the International Traffic in Arms Regulations.Prosecutors said Sun had been trained to handle the materials properly and knowingly transported the information to China without an export license, in violation of the AECA and the ITAR.The government did not present any evidence that Sun had personally supplied any sensitive information to Chinese government agents.

Web Notice: The Directorate of Defense Trade Controls (DDTC) is currently in the process of modernizing its IT systems. During this time period, we anticipate there may be delays in response times and time to resolve IT related incidents and requests. We apologize for any inconvenience, and appreciate your patience while we work to improve DDTC services. If you need assistance, please contact the DDTC Service Desk at (202) 663-2838, or email at DtradeHelpDesk@state.gov (06.28.16)

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.

Reproduction for private use or gain is subject to original copyright restrictions.