EIB World Trade Headlines

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

October 15, 2019 - Volume 11, Issue 20

US RETALIATES WITH EU TARIFF INCREASE ON EVERY DAY GOODS

The Trump administration plans to place tariffs on $7.5 billion worth of European imports — from gouda cheese to single-malt whiskey to large aircraft — beginning Oct. 18 to retaliate against illegal European Union subsidies for aviation giant Airbus.

The tariffs on EU imports will hit products including wine, olives, cheeses such as English cheddar and Swiss cheese and Irish butter such as Kerrygold, according to a list released by the United States Trade Representative. Liqueurs, cordials and Irish and Scotch whiskies will also face tariffs of 25%.

Rising tensions with Europe present a new headwind for the U.S. economy, which is losing speed amid the Trump administration's festering trade war with China and a weakening manufacturing sector. Earlier this week, a measure of factory activity in the U.S. registered its weakest reading in more than 10 years. Such concerns are making investors jittery, with the Dow closing down nearly 500 points on Wednesday and other leading indexes also losing ground.

"There is never a good time for the U.S. and the European Union to try to settle major trade disputes, particularly two as big as the Airbus/Boeing disputes. But this is the worst of times," said Kate Bronfenbrenner, senior lecturer at Cornell University's School of Industrial and Labor Relations, in an emailed statement.

*(*Continued On The Following Page)*

NEWSLETTER NOTES

She added, "The tariffs and counter tariffs will not only threaten hundreds of thousands of good union jobs in the airline industry but also jobs in the general manufacturing and agricultural sectors."

The European Union is expected to retaliate against the new U.S. tariffs, which are predicted to cause job losses, governments and industry groups said Thursday.

"We've tried to lessen this commercial tension, but if they are not in the mood for conciliation, obviously Europe will fight back," the French government's spokeswoman, Sibeth Ndiaye, told news broadcaster BFM TV.

WTO decision

The administration received a green light for its latest import taxes Wednesday from the World Trade Organization, which ruled that the United States could impose the tariffs as retaliation for illegal aid that the 28-country EU gave to Airbus in its competition with its American rival Boeing.

The WTO announcement culminates a 15-year fight over EU subsidies for Airbus.

EU aircraft will face a 10% import tax; other products on the list will be hit with 25% tariffs. The administration insists that it has the authority to increase the tariffs whenever it wants or to later the products in its list.

President Donald Trump called the WTO ruling a "big win for the United States" and asserted that it happened because WTO officials "want to make sure I'm happy. “The WTO has been much better to us since I've been president because they understand they can't get away with what they've been getting away with for so many years, which is ripping off the United States," Trump said at a joint White House news conference with President Sauli Niinisto of Finland.

Stock market losses

Stock markets around the world, which were already down on concerns for the world economy, added to their losses on the news.

Wednesday's award follows a WTO ruling in May 2018 that the EU had illegally helped Airbus with subsidies. It does not, however, end the long-running trans-Atlantic dispute over aircraft. WTO arbitrators are expected to rule next year about how much the EU can impose in tariffs following a separate decision that went against Boeing.

The EU's top trade official had said the bloc would prefer to reach a settlement with the United States to avoid a tariff war but that it will respond if Trump imposes new duties on EU products.

*(*Continued On The Following Column)*

Speaking after the WTO's ruling Wednesday but before the Trump administration announced the new tariffs, EU Trade Commissioner Cecilia Malmstrom said a tariff war "would only inflict damage on businesses and citizens on both sides of the Atlantic, and harm global trade and the broader aviation industry at a sensitive time."

"If the U.S. decides to impose WTO authorized countermeasures, it will be pushing the EU into a situation where we will have no other option than to do the same," she said.

"Defend our businesses"

Italian Foreign Minister Luigi Di Maio, who was meeting with U.S. Secretary of State Mike Pompeo in Rome on Wednesday, vowed to "defend our businesses." Italian wine and cheeses could face an impact from U.S. tariffs.

Unlike Trump's unilateral tariffs on billions of dollars-worth of steel, aluminum and other goods from China, the EU and elsewhere, the retaliatory tariffs authorized in the Airbus case have the stamp of approval from the WTO, an organization that he has repeatedly criticized.German Chancellor Angela Merkel acknowledged "we have lost a matter under WTO law."

"This means it's not some sort of arbitrary question but a verdict according to international law that now weighs on Airbus, one must sadly say," she told reporters in Berlin. "We have to see how the Americans will react now."

Airbus dispute

The WTO in May 2018 found that EU aid for Airbus had resulted in lost sales for Boeing in the twin-aisle and very large-aircraft markets. The ruling centered on Airbus' 350XWB — a rival of Boeing's 787 — and the double-decker A380, which tops the Boeing 747 as the world's largest commercial passenger plane. Airbus and Boeing dominate the market for large airliners, and Boeing's deliveries have plummeted this year because of the grounding of its 737 Max jet after two deadly crashes. This limits options for airlines looking to expand their fleets to accommodate increased air travel.

U.S. airlines have argued against tariffs on planes and parts that they buy from Europe, and they have mobilized supporters in Congress. In a letter this week to Trade Representative Robert Lighthizer, 34 congressional Republicans and Democrats expressed opposition to tariffs on imported airplanes and parts. And they suggested that if the tariffs were imposed that they apply only to future orders.The lawmakers noted that because aircraft orders usually stretch out years, it's hard for airlines to change or cancel them.

(*Continued On The Following Page)

Tariffs on European planes "would simply make these aircraft more expensive ... and would do nothing to encourage the EU to end the illegal subsidies," they wrote. By contrast, they said, imposing tariffs only on future orders from the EU would give airlines an incentive to buy U.S.-made planes.

A 15-year case

The case itself dates to 2004, a testament to the plodding and thorough rhythm of the Geneva-based trade body.

Rod Hunter, a partner at the law firm Baker McKenzie and a former White House economic official, saw three possible outcomes: The EU can end the offending subsidies to Airbus, decide to absorb the tariffs or try to reach a negotiated settlement with the Trump administration.

In a statement, Lighthizer said, "We expect to enter into negotiations with the European Union aimed at resolving this issue in a way that will benefit American workers."

The $7.5 billion represents a fraction of EU exports to the United States, which last year amounted to $688 billion.

But the specter of more tariffs comes at a sensitive time. Trump's aggressive use of tariffs _ especially against China _ has shaken financial markets, hobbled global trade and hurt manufacturers paralyzed with uncertainty about where to buy supplies, situate factories and sell their products. On Tuesday, a private index of U.S. manufacturing output dropped to its lowest level since the recession year 2009.

"The market effect could be larger than just the impact on the European exports and their U.S. customers,'' Hunter said.

Gary Hufbauer, a senior fellow at the Peterson Institute for International Economics and a former U.S. trade official, cast doubt on prospects for a EU-US trade deal that will ease tensions and ward off tit-for-tat tariffs, at least before the 2020 U.S. presidential election.

"Election years are bad for trade deals,'' Hufbauer said.

The WTO is already examining a dozen cases involving U.S. tariffs and countermeasures brought by its trading partners over the administration's steel and aluminum tariffs. Trump has insisted the move is needed to protect U.S. national security interests, but the Europeans claim it is simply protectionism and breaks global trade rules.

The EU has introduced "rebalancing" tariffs on about 2.8 billion euros ($3 billion) of U.S. steel, agricultural and other products. Trump has also threatened to slap duties on European automakers.

State Department clears five foreign military sales, including $3.3B interceptor deal for Japan

By Justin Doubleday
August 27, 2019 at 4:27 PM

The State Department notified Congress today of five potential foreign military sales, including a $3.3 billion deal with Japan for Standard Missile-3 Block IIA interceptors.

The possible sale to Japan includes 73 SM-3 Block IIA missiles, as well as associated Mk-29 cannisters and other support equipment, according to the Defense Security Cooperation Agency. Japan has co-developed the SM-3 Block IIA with the United States, involving an industry team of Mitsubishi Heavy Industries and Raytheon. Earlier this year, the Pentagon's top technology official directed an independent assessment of the SM-3 Block IIA before considering whether to transition the program to production.

Meanwhile, the State Department also approved of Lithuania purchasing 500 Joint Light Tactical Vehicles at an estimated cost of $170.8 million and Denmark buying Airborne Low Frequency Sonar Systems and Sonobuoys for an estimated $200 million, according to DSCA. Additionally, Hungary has been cleared for a potential $500 million purchase of AIM-120C-7 Advanced Medium-Range Air-to-Air Missiles, while South Korea has been approved to buy $72 million worth of MK-54 Lightweight Torpedoes, DSCA announced today.

North Korea Claims Its Underwater-Launched Missile Test Was Successful

Anna Kaplan Breaking News Reporter
Published 10.04.19 12:17AM ET

North Korea said it tested its underwater-launched ballistic missile for the first time in three years as nuclear diplomacy talks resume this weekend between the country and the United States. North Korea's state-run news agency KCNA said the missile test was successful and "ushered in a new phase in containing the outside forces' threat to [North Korea] and further bolstering its military muscle for self-defense." North Korea said the Pukguksong-3 missile is capable of being launched from a submarine, and the AP reports that Wednesday's test is seen as one of North Korea's most prominent weapons launches since it began diplomacy with the United States last year. KNCA did not report if the missile was fired from a submarine or another underwater launch platform, but the Pentagon said missile was not launched from a submarine. Joint Chiefs of Staff spokesman Air Force Col. Pat Ryder told Pentagon reporters Thursday that the missile was likely launched from a "sea-based platform.

Virgin Says Hyperloop Will Be the Best Mode of Transportation

Virgin Hyperloop One (VHO) believes it is sitting on the world's most efficient mode of transportation. The prediction came as the Los Angeles-based company also announced it is joining the Ellen MacArthur Foundation's CE [Circular Economy] 100 Network. The charity organization is dedicated to bringing public and private groups together in the name of accelerating innovations that will facilitate a circular economy – meaning one in which sustainability, recycling, and reduced waste are the norm.

In a press statement, Virgin Group founder Sir Richard Branson said that innovations like the hyperloop are going to be necessary to drive toward a more sustainable fufure while still meeting increasing demands for transportation. “The only way to address this mounting crisis is head-on,” Branson said. “We need big ideas like hyperloop to reach zero-emission transport while rapidly connecting people and goods.”

“As the world’s population grows, especially our urban populations, global demands for rapid, seamless travel, and more efficient deliveries will continue to rise. We must meet demand in a way that is efficient, clean, and protects the future of our planet,” Jay Walder, CEO of VHO, added. “Hyperloop technology can be that radical solution, setting the bar for the fastest, most energy-efficient, and sustainable form of travel ever created.”

A conceptual rendering of hyperloops deployed for cargo shipping. (Image source: Virgin Hyperloop One)

VHO says its hyperloop technology, which uses magnetic levitation to propel a capsule-like vehicle through a depressurized tube, can transport humans and goods at nearly 700 miles per hour. “It will be able to carry more people than a subway, at airline speeds and with zero direct emissions,” the company said.

*(*Continued On The Following Column)*

“By combining an ultra-efficient electric motor, magnetic levitation, and a low-drag environment, the VHO system will be five to 10 times more energy-efficient than an airplane and faster than high-speed rail using less energy.” Further, the company proposes that solar panels can be integrated into the hyperloop's infrastructure to provide for its energy needs.

VHO is currently on a tour across America. The Hyperloop Progress & American Roadshow has been touring major cities across the US to introduce the public to hyperloop technology, specifically the company's XP-1 vehicle. The company also has several hyperloop projects underway across the country. The Dallas-Fort Worth Regional Transportation Council and The Mid-Ohio Regional Planning Commission are conducting active feasibility studies into the environmental impact of the hyperloop and the viability of building hyperloop routes in the Fort Worth area and the Chicago-Columbus-Pittsburgh corridor respectively. VHO also maintains a working test site in Nevada called DevLoop.

Internationally, the company is currently working with the Indian government of Maharashtra on developing a hyperloop route between Pune and Mumbai. “The implementation of a regional VHO system could reduce local greenhouse gas emissions by up to 150,000 tons (300 million pounds) annually while creating 1.8 million new jobs and $36 billion in economic impact across the region,” according to VHO.

An Open-Source Transportation Innovation

The idea of the hyperloop was first proposed by Tesla and SpaceX CEO Elon Musk, circa 2012. Musk's vision was for a new form of transportation that would be immune to weather changes, consume very little energy, never have collisions, store enough energy to operate 24/7, and travel at high speeds (able to travel from Los Angeles to San Francisco in 30 minutes).

VHO's XP-1 at the company's DevLoop test track in Nevada. (Image source: Virgin Hyperloop One)

(*Continued On The Following Page)

The concept was to place pods inside of a tube that contained an array of fans. The fans would create a partial vacuum within the tube, allowing the pods to be propelled (via wheels, air pressure, electromagnetic propulsion, or some other means) through the tube at high speeds. Enthusiasts believe the hyperloop could one day obtain supersonic speeds.

In 2013 engineers at Tesla and SpaceX released a 57-page white paper detailing an early design concept. That same year Musk announced he was open-sourcing the concept so that other companies and institutions could iterate on the idea and speed its development. This has led to a small ecosystem of hyperloop companies like VHO, Los Angeles-based Hyperloop Transportation Technologies, and Canadian company Transpod to emerge.

There have also been competitions challenging students and startups to develop their own hyperloop solutions. Design News chronicled the journey of one of those teams – Team rLoop. that created its own hyperloop system entirely via social media collaboration.

The Long Loop Ahead

All of this is not to say that hyperloop technology has a smooth road (or tube) ahead. There have yet to be any tests or deployments on the scale comparable to even a short commercial flight. And there are a lot of questions around the logistics necessary to implement a large-scale hyperloop infrastructure.

A 2019 report, “Global Hyper loop Technology Market Research Report- Forecast 2023” published by Market Research Future predicted that transportation demands point to potential growth in the hyperloop market but also that the technology faces major obstacles.

The “possibility of technical glitches and the shortage of power restrain the market growth,” the report said. “Other restraints could be that terrain and other natural disasters will act as a major restraint for this market. In addition to this, it is seen that the online services connected with hyperloop will require connection to the pods which might affect the magnetic field within the tube further forming a major obstacle for the implementation process.”

Chris Wiltz is a Senior Editor at Design News covering emerging technologies including AI, VR/AR, blockchain, and robotics.

Understanding NIST 800-171 Impact on Acquisition

By Casey Lang • November 13, 2017

Thanks to the increasingly sophisticated and aggressive cybersecurity threats facing the U.S., there has been much focus recently on reinforcing the nation’s cybersecurity. Much of this effort has revolved around strengthening the Department of Defense (DoD) supply chain.
The Defense Federal Acquisition Regulation Supplement, or DFARS, has been working to encourage DoD contractors to proactively comply with certain frameworks in order to achieve this goal. Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is the latest mandatory addition.

Under the Clause, all contractors must comply with the National Institute of Standards and Technology’s Special Publication 800-171 (NIST SP 800-171), a framework that lays out how contractors must protect sensitive defense information and report cybersecurity incidents.

The NIST framework requires you, as a defense contractor, to document how you have met the following requirements in particular:

• Security requirement 3.12.4 requires the contractor to develop, document, and periodically update System Security Plans (SSPs) that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
• Security Requirement 3.12.2 requires the contractor to develop and implement Plans of Action designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems.

As a contractor, you need to safeguard covered defense information that is processed or stored on your internal information system or network.

To stay in the running for work from your primes, you need to comply with DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, which requires contractors to implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations”. You have until December 31, 20 I 7 to implement NIST SP 800-171.

*(*Continued On The Following Page)*

How will non-compliance with NIST SP 800-171 impact contractors' future acquisition?

On September 21, 2017, The Director, Defense Pricing/Defense Procurement and Acquisition Policy issued guidance for acquisition personnel in anticipation of the December 31, 2017 deadline, which:

Outlines how contractors might implement NIST SP 800-171.
Addresses how a contractor may use a system security plan to document the implementation of the NIST SP 800-171 security requirements.
Describes how DoD organizations might choose to leverage the contractor's system security plan (SSP), and any associated plans of action, in the contract formation, administration, and source selection processes.
To not jeopardize future opportunities, contractors should focus on developing a well-written SSP and associated Plan of Action and Milestones (POA&M) to achieve compliance.

What are the SSP and POA&M requirements?

NIST SP 800-171 was revised (Revision 1) in December 2016 to require a "system security plan" and associated "plans of action." Specifically:

Security requirement 3.12.4 (System Security Plan, added by NIST SP 800-171, Revision 1), requires the contractor to develop, document, and periodically update, system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
Security Requirement 3.12.2 (Plans of Action), requires the contractor to develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems.
How do you write an SSP and POA&M?

Documenting implementation of the NIST SP 800-171 security requirements by the December 31, 2017, implementation deadline requires an SSP and associated plans of action which describe how and when you will meet unimplemented security requirements, how you will implement planned mitigations, and how and when you will correct deficiencies and reduce or eliminate vulnerabilities in the systems. System security plans and plans of action can be documented as separate or combined documents. You should choose a format that integrates with existing business processes and can be easily maintained year-over-year. Governance, Risk, and Compliance platforms can provide a technical, somewhat automated capability to meet this objective.

*(*Continued On The Following Column)*

There is no prescribed methodology for contractors to implement the requirements of NIST SP 800-171, or even to assess your current compliance with the requirements -nor is there a prescribed format for SSPs or POA&Ms. A reasonable first step in creating an SSP and POA&M is to use company personnel or a qualified third party to execute a gap assessment against current operations compared to the NIST SP 800-171 requirements. The gap assessment will detail changes to policy and highlight areas where additional hardware or software are required to achieve compliance. A well-executed gap assessment will determine:

Requirements that can be met using in-house IT personnel.
Requirements that can be met using outside assistance.
Plan of Action and Milestones for achieving compliance.
Which version of NIST 800-171 applies?

DFARS Clause 252.204-7012 requires the contractor to implement the version of the NIST SP 800-171 that is in effect at the time of the solicitation, or such other version that is authorized by the contracting officer.

How do you inform the Government of compliance with NIST SP 800-171 requirements?

You can inform the Government of your implementation of the NIST SP 800-171 requirements in a number of ways.

The solicitation provision DFARS 252.204-7008, "Compliance with Safeguarding Covered Defense Information Controls," provides that by submitting the offer, the contractor is representing its compliance (and provides a procedure for the contractor to request the DoD Chief Information Officer (CIO) to authorize a variance from any of those requirements as being non-applicable, or because the contractor has a different but equally effective security measure).
Paragraph (c)(2)(ii)(A) of DFARS Clause 252.204-7012 requires the contractor that is performing a contract awarded prior to October 1, 2017, to notify the DoD CIO of any requirements of NIST SP 800-171 that are not implemented at the time of contract award.
Keep in mind, the solicitation may require or allow elements of the system security plan, which documents the implementation of NIST SP 800-171, to be included with your technical proposal, and may be incorporated as part of the contract (e.g., via a Section H special contract requirement).

What is the role of the SSP and POA&M in contract formulation, administration, and source selection?

Chapter 3 of NIST SP 800-171, Revision 1, states that Federal agencies may consider the contractor's system security plan and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization, and whether or not it is advisable to pursue an agreement or contract with the nonfederal organization.

(*Continued On The Following Page)

DFARS Clause 252.204-7012 is not structured to require contractor implementation of NIST SP 800-171 as a mandatory evaluation factor in the source selection process, but the requiring activity is not precluded from using a company's SSP and associated POA&Ms to evaluate the overall risk introduced by the state of the contractor's internal information system or network.

The Director, Defense Pricing/Defense Procurement and Acquisition Policy guidance for acquisition personnel provide the following examples of how the government may utilize the system security plan and associated plans of action:

Using proposal instructions and corresponding evaluation specifics (detailed in sections L and M of the solicitation as well as the Source Selection Plan) regarding how implementation of NIST SP 800-171 (and other applicable security measures) will be used by DoD to determine whether it is an acceptable or unacceptable risk to process, store, or transmit covered defense information on a system hosted by the offeror. The solicitation must notify the offeror whether and how its approach to protecting covered defense information and providing adequate security in accordance with DFARS 252.204-7012 will be evaluated in the solicitation. Establishing compliance with DFARS 252.204-7012 as a separate technical evaluation factor and notifying the offeror that its approach to providing adequate security will be evaluated in the source selection process. The specifics of how the offeror's implementation of NIST SP 800-171 will be evaluated must be detailed in Sections L and M of the solicitation as well as the Source Selection Plan.

https://cybersheath.com/understanding-nist-800-171-impact-acquisition/

America Misses the Free-Trade Wave

While the US pursues a trade war and levies tariffs on allies, the rest of the world is undergoing a free-trade renaissance, Shannon K. O'Neil writes at Bloomberg. Asian countries enjoy market access after coming up with a replacement for the Trans-Pacific Partnership; Africa is working toward a new free-trade zone, Latin America's Pacific Alliance trade bloc of Chile, Colombia, Mexico, and Peru is looking to expand its reach; and Japan struck a deal with the EU.

As a result, other countries are poised to set new trade rules in America's absence, O'Neil writes. "When historians look back, they may depict this as a time when free traders set new rules for decades to follow," O'Neil writes—and if the US stays on the sidelines, it won't have a say.

Airline Stocks: US Levies 10% Tariffs on Airbus Aircraft

Airline stocks could be in focus today, as the Trump administration has levied a hefty tariff on European-made Airbus aircraft. The latest move came after the WTO (World Trade Organization) ruled in the US's favor in a 15-year old dispute regarding Airbus. Yesterday morning, the WTO found the EU guilty of providing unfair subsidies to the European planemaker. The ruling paved the way for the US to quickly impose tariffs on European-made goods worth $7.5 billion. Yesterday, Reuters reported the government had released a list of hundreds of European commodities that will be tariffed. Washington has imposed 25% import duties on Italian cheese, single malt whisky, and French wine. The list also includes UK-made blankets and German camera parts. However, the main target was Airbus aircraft.

The US government is enforcing a 10% duty on aircraft imported from Airbus's European facilities. The new tariffs on European products are set to take effect on October 18. The tariffs could severely hurt US airlines, as they're set to make Airbus planes costlier. Most US carriers have pending Airbus orders worth billions of dollars. As of August 31, Delta Air Lines (DAL) had 254 unfulfilled orders with the European aircraft manufacturer. Meanwhile, American Airlines (AAL) is awaiting 114 Airbus deliveries. United Airlines (UAL) and JetBlue (JBLU) have 45 and 154 unfulfilled orders, respectively.

Therefore, airlines were the most beaten-down stocks during yesterday's sell-off after the WTO's ruling. With a 5.3% intraday decline, American Airlines plunged the most. United followed, falling 4.7%. Delta and JetBlue closed 4.7% and 2.5% lower, respectively. The Dow Jones Transportation Average fell 235 points, or 2.3%, yesterday. All 20 of its components closed in the red.

The tariffs on European-made aircraft put US airlines at more risk. Together, Airbus and Boeing (BA) hold over 90% of the commercial airplane manufacturing space. As Airbus planes become more expensive, US airlines could have less bargaining power with Boeing.

The WTO also found the US guilty in a similar case the EU filed regarding Boeing. The final ruling could come in early January, and it looks like it could be in the EU's favor. Therefore, the EU could retaliate with levying hefty charges on US-made goods. Following the WTO ruling, European trade commissioner Cecilia Malmström said, "If the U.S. decides to impose WTO authorized countermeasures, it will be pushing the EU into a situation where we will have no other option than do the same," according to CNBC. The latest tariffs escalate the US-EU trade war. The EU is already facing 25% and 10% duties on steel and aluminum exports. Furthermore, the Trump administration intends to tariff European-made cars and parts. On the other hand, the EU has enforced duties on $3 billion in US imported goods.

Citizen of Singapore indicted in scheme to steal cloud computing power for cryptocurrency mining

Department of Justice
U.S. Attorney's Office
Western District of Washington
FOR IMMEDIATE RELEASE
Wednesday, October 9, 2019

Masqueraded as California video game developer to access cloud computing services

Seattle - A 14-count indictment was unsealed today charging a citizen of Singapore, HO JUN JIA, a/k/a Matthew Ho, 29, with federal crimes related to his scheme to mine cryptocurrencies using stolen computing power and services, obtained with the stolen identity and credit card account information of California and Texas residents, announced U.S. Attorney Brian T. Moran.

HO was taken into custody by the Singapore Police Force on September 26, 2019, and is being investigated for various alleged offenses committed under Singapore law.

According to the indictment, between October 2017 and February 2018, following the surge in popularity, and value, of cryptocurrencies, HO ran a large-scale cryptocurrency mining operation, propelled predominantly, if not exclusively, through fraud and identity theft.

HO, allegedly used stolen identity and credit card information of a prominent California video-game developer to open cloud computing accounts at multiple U.S. cloud service providers, which he used to mine various cryptocurrencies, such as Bitcoin and Ethereum. HO created a web of phony email accounts and used social engineering techniques to trick cloud computing providers to approve heightened account privileges, increased computer processing power and storage, and deferred billing.

HO used the fraudulently obtained computing power to mine cryptocurrency – a resource-intensive process by which "miners" essentially compete to verify blockchain transactions and receive an amount of cryptocurrency in return. HO then used the cryptocurrency or exchanged it for traditional funds on various marketplace websites. In the few months his scheme remained active, HO consumed more than $5 million in unpaid cloud computing services with his mining operation and, for a brief period, was one of Amazon Web Services (AWS) largest consumers of data usage by volume. Some of the bills were paid by the California game developer's financial staff before the fraud was detected.

*(*Continued On The Following Column)*

HO used the fraudulently obtained computing power to mine cryptocurrency – a resource-intensive process by which "miners" essentially compete to verify blockchain transactions and receive an amount of cryptocurrency in return. HO then used the cryptocurrency or exchanged it for traditional funds on various marketplace websites. In the few months his scheme remained active, HO consumed more than $5 million in unpaid cloud computing services with his mining operation and, for a brief period, was one of Amazon Web Services (AWS) largest consumers of data usage by volume. Some of the bills were paid by the California game developer's financial staff before the fraud was detected. HO also used the identities of a Texas resident and the founder of a tech company in India and, in addition to AWS, opened cloud services accounts with Google Cloud Services, which he similarly used as part of his cryptocurrency mining operation.

Wire fraud is punishable by up to 20 years in prison. Access device fraud is punishable by up to ten years in prison. Aggravated identity theft is punishable by a mandatory two years in prison to run consecutive to any other sentence imposed in the case.

The charges contained in the indictment are only allegations. A person is presumed innocent unless and until he or she is proven guilty beyond a reasonable doubt in a court of law.

The case is being investigated by the FBI Seattle Office, Cyber Crime Unit, with assistance from the Singapore Police Force - Technology Crime Investigation Branch, the Attorney General's Chambers of Singapore, the U.S. Department of Justice's Criminal Division's Office of International Affairs, and the FBI Legal Attaché Office.

The case is being prosecuted by Assistant United States Attorney Steven Masada.

Posed photo of a hacker. The suspect allegedly ran a large-scale cryptocurrency mining operation, propelled predominantly, if not exclusively, through fraud and identity theft.PHOTO: REUTERS

ENFORCEMENT INFORMATION FOR OCTOBER 1, 2019

Information concerning the civil penalties process can be found in the Office of Foreign Assets Control (OFAC) regulations governing each sanctions program; the Reporting, Procedures, and Penalties Regulations, 31 C.F.R. part 501; and the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A. These references, as well as recent final civil penalties and enforcement information, can be found on OFAC's website at www.treasury.gov/ofac/enforcement.

ENTITIES - 31 C.F.R. 501.805(d)(1)(i)

The General Electric Company Settles Potential Civil Liability for Alleged Violations of the Cuban Assets Control Regulations: The General Electric Company ("GE") of Boston, Massachusetts, on behalf of three current and former GE subsidiaries, Getsco Technical Services Inc., Bentley Nevada, and GE Betz (collectively, the "GE Companies"), has agreed to pay $2,718,581 to settle its potential civil liability for 289 alleged violations of the Cuban Assets Control Regulations, 31 C.F.R. part 515 (CACR). Specifically, between December 2010 and February 2014, the GE Companies appear to have violated § 515.201(b) of the CACR on 289 occasions by accepting payment from The Cobalt Refinery Company ("Cobalt") for goods and services provided to a Canadian customer of GE.

Since June 1995, Cobalt had been identified as a specially designated national (SDN) of Cuba and appeared on OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List"). Publicly available information also demonstrated that GE's former Canadian customer is a corporation with strong historic and then-current economic ties to the Cuban mining industry through its business partnerships and joint ventures with the Cuban government. Cobalt is one of three entities owned by a public joint venture between GE's Canadian customer and the Cuban government. From at least 1996 until the GE Companies terminated their relationship with their Canadian customer, the GE Companies maintained — and renewed on at least 18 occasions — this customer relationship despite the obvious sanctions risk posed by the relationship.

On February 24, 2014, GE Working Capital Solutions discovered that from at least 2010 to 2014, the GE Companies received numerous payments directly from Cobalt for invoices issued to GE's Canadian customer. While the GE Companies negotiated and entered into contracts with GE's Canadian customer, and sent all of their invoices to GE's Canadian customer, Cobalt paid the GE Companies for its goods and services in more than 65 percent of the total transactions. The GE Companies approved Cobalt as a third-party payer and, over a four-year period, failed to appropriately recognize the significant and widely published relationship between Cobalt and their Canadian customer and did not undertake sufficient diligence into their customer's activities.

*(*Continued On The Following Column)*

The GE Companies deposited all checks received from Cobalt into GE's bank account at a Canadian financial institution. The checks contained Cobalt's full legal entity name as it appears on OFAC's SDN List as well as an acronym for Cobalt ("Corefco"), but the GE Companies' sanctions screening software, which screened only the abbreviation of the SDN's name, never alerted on Cobalt's name. In total, the GE Companies received 289 checks directly from Cobalt from on or about December 9, 2010 to on or about February 28, 2014 totaling approximately $8,018,615.

Additionally, goods and services the GE Companies provided to its Canadian customer were, in turn, used to supply utility services and other benefits to Cobalt, which is co-located with GE's Canadian customer. The statutory maximum civil monetary penalty applicable in this matter is $18,785,000. OFAC determined, however, that GE voluntarily self-disclosed the alleged violations, and that the alleged violations constitute a non-egregious case. Accordingly, under OFAC's Economic Sanctions Enforcement Guidelines ("Enforcement Guidelines"), the base civil monetary penalty amount applicable in this matter is $3,377,119. The settlement amount of $2,718,581 also reflects OFAC's consideration of the General Factors under the Enforcement Guidelines. Specifically, OFAC determined the following to be aggravating factors:

(1) The GE Companies failed to take proper or reasonable care with respect to their U.S. economic sanctions obligations — particularly given GE's commercial sophistication. GE failed to identify that (i) for at least four years it was receiving payments that were on their face from a SDN of Cuba that has been on the SDN List since 1995, and (ii) it was providing goods and services to a customer that provides a direct and indirect benefit to a facility owned and operated by that designated Cuban company;

(2) The GE Companies' actions caused substantial harm to the objectives of the Cuba sanctions program by conducting a large volume of high-value transactions directly with a Cuban company on the SDN List over a period of many years; and

(3) The substance of GE's disclosures and other communications with OFAC leave substantial uncertainty about the totality of the benefits conferred to a Cuban company on the SDN List by the GE Companies through their Canadian customer, which had substantial and public ties to Cuba and the Cuban mining industry. While OFAC considered certain jurisdictional limitations on GE's ability to provide a full picture of the scope of work performed at the request of its Canadian customer, at all relevant times, GE had reason to know of its customer's specific and longstanding relationship with Cobalt. GE should have treated its Canadian customer as higher risk due to the customer's publicly known joint venture with Cuba and substantial reliance on Cuban-origin ore.

*(*Continued On The Following Page)*

Finally, despite the provision to GE of OFAC's Office of Enforcement Data Delivery Standards, GE did not provide its primary submissions to OFAC in a clear and organized manner and the submissions contained numerous inaccuracies, placing a substantial resource burden on OFAC during the course of its investigation.

OFAC determined the following to be mitigating factors:

(1) None of the GE Companies has received a penalty notice or Finding of Violation from OFAC in the five years preceding the date of the earliest transaction giving rise to the alleged violations;

(2) GE identified the alleged violations by testing and auditing its compliance program. Additionally, GE implemented remedial measures and new processes to enhance its sanctions compliance procedures, including developing a training video for all company employees using the alleged violations as a case study; and

(3) GE cooperated with OFAC by executing and extending multiple statute of limitations tolling agreements.

This enforcement action highlights the sanctions risks to U.S. companies and their foreign subsidiaries associated with (i) accepting payments from third parties and (ii) conducting transactions in foreign currency or at a foreign financial institution. Additionally, this action demonstrates the importance of conducting appropriate due diligence on customers and other counter-parties when *initiating* and *renewing* customer relationships. Ongoing compliance measures should be taken throughout the life of commercial relationships.

As noted in OFAC's Framework for Compliance Commitments, U.S. companies can mitigate sanctions risk by conducting risk assessments and exercising caution when doing business with entities that are affiliated with, or known to transact with, OFAC-sanctioned persons or jurisdictions, or that otherwise pose high risks due to their joint ventures, affiliates, subsidiaries, customers, suppliers, geographic location, or the products and services they offer.

For more information regarding OFAC regulations, please go to: *www.treasury.gov/ofac*.

New Entities Added to Entities List

ERC Entity List Decisions Additions to the Entity List

This rule implements the decision of the ERC to add twenty-eight entities to the Entity List. The twenty-eight entities are being added based on § 744.11 (License requirements that apply to entities acting contrary to the national security or foreign policy interests of the United States) of the EAR. The twenty-eight entries are located in China.

The ERC reviewed and applied § 744.11(b) (Criteria for revising the Entity List) in making the determination to add these twenty-eight entities to the Entity List. Under that paragraph, persons for whom there is reasonable cause to believe, based on specific and articulable facts, that they have been involved, are involved, or pose a significant risk of being or becoming involved in activities that are contrary to the national security or foreign policy interests of the United States, along with those acting on behalf of such persons, may be added to the Entity List. Paragraphs (b)(1) through (b)(5) of § 744.11 provide an illustrative list of activities that could be contrary to the national security or foreign policy interests of the United States. For each of the twenty-eight entities described below, the ERC made the requisite determination under the standard set forth in § 744.11(b).

Pursuant to § 744.11(b) of the EAR, the ERC determined that the Xinjiang Uighur Autonomous Region (XUAR) People's Government Public Security Bureau, eighteen of its subordinate municipal and county public security bureaus and one other subordinate institute are engaging in activities contrary to the foreign policy interests of the United States, and eight additional entities are enabling activities contrary to the foreign policy interests of the United States. Specifically, these entities have been implicated in human rights violations and abuses in the implementation of China's campaign of repression, mass arbitrary detention, and high-technology surveillance against Uighurs, Kazakhs, and other members of Muslim minority groups in the XUAR.

The entities are as follows: Xinjiang Uighur Autonomous Region (XUAR) People's Government Public Security Bureau, eighteen of its subordinate municipal and county public security bureaus, and one other subordinate institute:—Aksu District Public SecurityBureau; Altay Municipality Public Security Bureau; Bayingolin Mongolian Autonomous Prefecture Public Security Bureau; Boertala Mongolian Autonomous Prefecture Public Security Bureau; Changji Hui Autonomous Prefecture Public Security Bureau; Hami Municipality Public Security Bureau;

(*Continued On The Following Page)

Hetian Prefecture Public Security Bureau; Kashgar Prefecture Public Security Bureau; Kelamayi Municipality Public Security Bureau; Kezilesu Kyrgyz Autonomous Prefecture Public Security Bureau; Shihezi Municipality Public Security Bureau; Tacheng Prefecture Public Security Bureau; Tumushuke Municipal Public Security Bureau; Turfan Municipality Public Security Bureau; Urumqi Municipal Public Security Bureau; Wujiaqu Municipality Public Security Bureau; Xinjiang Police College; Xinjiang Production and Construction Corps (XPCC) Public Security Bureau; and Yili Kazakh Autonomous Prefecture Public Security Bureau.
The following eight entities are also added to the Entity List as part of this rule: Dahua Technology; Hikvision; IFLYTEK; Megvii Technology; Sense Time, Xiamen Meiya Pico Information Co. Ltd.; Yitu Technologies; and Yixin Science and Technology Co. Ltd. Pursuant to § 744.11(b) of the EAR, the ERC has determined that the conduct of these twenty-eight entities raises sufficient concern that prior review of exports, reexports or transfers (incountry) of all items subject to the EAR involving these entities, and the possible imposition of license conditions or license denials on shipments to the persons, will enhance BIS's ability to prevent items subject to the EAR from being used in activities contrary to the foreign policy of the United States.

For the twenty-eight entities described above that are being added to the Entity List, BIS imposes a license requirement for all items subject to the EAR and a license review policy of case-by- case review for Export Control Classification Numbers (ECCNs) 1A004.c, 1A004.d, 1A995, 1A999.a, 1D003, 2A983, 2D983, and 2E983. A policy of case-by-case review also applies to items designated as EAR99 that are described in the Note to ECCN 1A995, specifically, items for protection against chemical or biological agents that are consumer goods, packaged for retail sale or personal use, or medical products. BIS has adopted a license review policy of presumption of denial for all other items subject to the EAR.

For all twenty-eight entities, the license requirements apply to any transaction in which items are to be exported, reexported, or transferred (in country) to any of the entities or in which such entities act as purchaser, intermediate consignee, ultimate consignee, or end user. In addition, no license exceptions are available for exports, reexports, or transfers (in-country) to the entities being added to the Entity List in this rule. The acronym ''a.k.a.'' or also known as is used in entries on the Entity List to identify aliases, thereby assisting exporters, reexporters and transferors in identifying entities on the Entity List.

*(*Continued On The Following Column)*

This final rule adds the following twenty-eight entities to the Entity List and includes, where appropriate, aliases: People's Republic of China

- Aksu District Public Security Bureau, including one alias (Aqsu District Public Security Bureau);
- Altay Municipality Public Security Bureau;
- Bayingolin Mongolian Autonomous Prefecture Public Security Bureau;
- Boertala Mongolian Autonomous Prefecture Public Security Bureau, including one alias (Bortala Mongolian Autonomous Prefecture Public Security Bureau);
- Changji Hui Autonomous Prefecture Public Security Bureau;
- Dahua Technology;
- Hami Municipality Public Security Bureau, including two aliases (Kumul Municipality Public Security Bureau; and Qumul Municipality Public Security Bureau);
- Hetian Prefecture Public Security Bureau;
- Hikvision;
- IFLYTEK;
- Kashgar Prefecture Public Security Bureau;
- Kelamayi Municipality Public Security Bureau;
- Kezilesu Kyrgyz Autonomous Prefecture Public Security Bureau, including one alias (Kizilsu Autonomous Prefecture Public Security Bureau);
- Megvii Technology;
- Sense Time;
- Shihezi Municipality Public Security Bureau;
- Tacheng Prefecture Public Security Bureau;
- Tumushuke Municipal Public Security Bureau, including one alias (Tumxuk Municipal Public Security Bureau);
- Turfan Municipality Public Security Bureau, including one alias (Turpan Municipality Public Security Bureau);
- Urumqi Municipal Public Security Bureau;

*(*Continued On The Following Page)*

• Wujiaqu Municipality Public Security Bureau;

• Xiamen Meiya Pico Information Co. Ltd.;

• Xinjiang Police College;

• Xinjiang Production and Construction Corps (XPCC) Public Security Bureau;

• Xinjiang Uighur Autonomous Region (XUAR) People's Government Public Security Bureau;

• Yili Kazakh Autonomous Prefecture Public Security Bureau, including one alias (Ili Kazakh Autonomous Prefecture Public Security Bureau);

• Yitu Technologies;

• Yixin Science and Technology Co. Ltd., including four aliases (Yixin Technology; Yuxin Technology; Yuxin Science and Technology; and Ecguard).

Savings Clause Shipments of items removed from eligibility for a License Exception or for export or reexport without a license (NLR) as a result of this regulatory action that were en route aboard a carrier to a port of export or reexport, on October 9, 2019, pursuant to actual orders for export or reexport to a foreign destination, may proceed to that destination under the previous eligibility for a License Exception or export or reexport without a license (NLR).

Export Control Reform Act of 2018 On August 13, 2018, the President signed into law the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which included the Export Control Reform Act of 2018 (ECRA) (50 U.S.C. 4801–4852) that provides the legal basis for BIS's principal authorities and serves as the authority under which BIS issues this rule. As set forth in Section 1768 of ECRA, all delegations, rules, regulations, orders, determinations, licenses, or other forms of administrative action that have been made, issued, conducted, or allowed to become effective under the Export Administration Act of 1979 (50 U.S.C. 4601 et seq.) (as in effect prior to August 13, 2018 and as continued in effect pursuant to the International Emergency

*(*Continued On The Following Column)*

"Your only limit is you."

Economic Powers Act (50 U.S.C. 1701 et seq.) and Executive Order 13222 of August 17, 2001, 3 CFR, 2001 Comp., p. 783 (2002), as amended by Executive Order 13637 of March 8, 2013, 78 FR 16129 (March 13, 2013), and as extended by the Notice of August 14, 2019, 84 FR 41881 (August 15, 2019)), or the

Export Administration Regulations, and are in effect as of August 13, 2018, shall continue in effect according to their terms until modified, superseded, set aside, or revoked under the authority of ECRA.

Tariffs China

More red warning lights are flashing for the economy. American manufacturing had its worst month in over a decade. A closely watched report says manufacturing activity dropped in September to a level not since June 2009, the month the Great Recession ended. Economists blamed the trade war with China for the manufacturing decline. The Dow took it hard, dropping nearly 350 points. President Trump blamed the Federal Reserve