EIB World Trade Headlines

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

February 1, 2023 – Volume 18, Issue 3

DECCS User Group for 2023

DDTC is excited to announce the enrollment period is open for the 2023 DECCS User Group

What is it?

- The mission of the Defense Export Controls and Compliance System (DECCS) User Group (DUG) is to allow individual industry users to provide feedback on DECCS by establishing and maintaining a forum for active and regular communication between DECCS users and the Directorate of Defense Trade Controls (DDTC).
- DUG members will have the opportunity to:
  - Identify functional and technical challenges when interacting with DECCS, and
  - Provide feedback and input for future DECCS enhancements and system support initiatives.

Who should be involved?

- DDTC is looking for a diverse group of up to 50 industry volunteers (representatives of companies, government agencies and third-party organizations) enrolled with DECCS who can provide the end-user point-of-view on issues related to the system.
- Open to U.S.-based and international members.

What is the time commitment?

- DDTC plans to engage with DUG volunteers when there is system functionality ready for User Acceptance Testing. Time will vary based on testing requested. In total, time will not exceed 20 hours.
- Participation in the DUG Spring and Fall meetings.
- The DUG User Group term will span one calendar year.

How to get involved:

- To express your interest, email PM_DDTCProjectTeam@state.gov by COB February 28, 2023 and provide your name & company/government affiliation (as applicable)
- DDTC will inform applicants by March 31, 2023 on DUG membership selection

NEWSLETTER NOTES

DEPARTMENT OF THE TREASURY WASHINGTON, D.C.
OFFICE OF FOREIGN ASSETS CONTROL

Russian Harmful Foreign Activities Sanctions Regulations 31 CFR part 587

GENERAL LICENSE NO. 6C

Transactions Related to Agricultural Commodities, Medicine, Medical Devices, Replacement Parts and Components, or Software Updates, the Coronavirus Disease 2019 (COVID-19) Pandemic, or Clinical Trials

(a) Except as provided in paragraph (c) of this general license, all transactions prohibited by the Russian Harmful Foreign Activities Sanctions Regulations, 31 CFR part 587, related to: (1) the production, manufacturing, sale, transport, or provision of agricultural commodities, agricultural equipment, medicine, medical devices, replacement parts and components for medical devices, or software updates for medical devices; (2) the prevention, diagnosis, or treatment of COVID-19 (including research or clinical studies relating to COVID-19); or
(3) clinical trials and other medical research activities are authorized.
(b) For the purposes of this general license, agricultural commodities, medicine, and medical devices are defined as follows:
(1) Agricultural commodities. For the purposes of this general license, agricultural commodities are products that fall within the term "agricultural commodity" as defined in section 102 of the Agricultural Trade Act of 1978 (7 U.S.C. 5602) and are intended for use as:
(i) Food for humans (including raw, processed, and packaged foods; live animals; vitamins and minerals; food additives or supplements; and bottled drinking water) or animals (including animal feeds);
(ii) Seeds for food crops;
(iii) Fertilizers or organic fertilizers; or
(iv) Reproductive materials (such as live animals, fertilized eggs, embryos, and semen) for the production of food animals.
(2) Medicine. For the purposes of this general license, medicine is an item that falls within the definition of the term "drug" in section 201 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321).
(3) Medical devices. For the purposes of this general license, a medical device is an item that falls within the definition of "device" in section 201 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321).

(c) This general license does not authorize:
(1) The opening or maintaining of a correspondent account or payable-through account for or on behalf of any entity subject to Directive 2 under Executive Order (E.O.) 14024, *Prohibitions Related to Correspondent or Payable-Through Accounts and Processing of Transactions Involving Certain Foreign Financial Institutions*;
(2) Any debit to an account on the books of a U.S. financial institution of the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, or the Ministry of Finance of the Russian Federation; or
(3) Transactions prohibited by E.O. 14066, E.O. 14068, or E.O. 14071, except for transactions prohibited solely by the determination of May 8, 2022, made pursuant to section 1(a)(ii) of E.O. 14071, "Prohibitions Related to Certain Accounting, Trust and Corporate Formation, and Management Consulting Services".
(d) Effective January 17, 2023, General License No. 6B, dated July 14, 2022, is replaced and superseded in its entirety by this General License No. 6C.

Note 1 to General License No. 6C. Transactions prohibited by E.O. 14066, E.O. 14068, and E.O. 14071 include new investment in the Russian Federation and the importation into the United States of certain products of Russian Federation origin, such as alcoholic beverages and fish, seafood, or preparations thereof.

(*Continued On The Following Page)

Note 2 to General License No. 6C. Nothing in this general license relieves any person from compliance with any other Federal laws or requirements of other Federal agencies.

Dated: January 17, 2023

_____

Andrea M. Gacki
Director
Office of Foreign Assets Control

****

NEW AI AP

Attracting more than a million users within days of its release in November, ChatGPT—the new artificial-intelligence application from the U.S. research lab OpenAI—has provoked intensive global media coverage in the month and a half since. Responses to the technology—which can generate sophisticated written replies to complex questions; produce essays, poems, and jokes; and even imitate the prose styles of famous authors—have ranged from bemused astonishment to real anxiety: The New York Times tech columnist Kevin Roose wrote that "ChatGPT is, quite simply, the best artificial intelligence chatbot ever released to the general public"—while Elon Musk tweeted, "ChatGPT is scary good. We are not far from dangerously strong AI." Critics worry about the technology's potential to replace human work, enable student cheating, and disrupt the world in potentially countless other ways. What to make of it?

Sarah Myers West is the managing director of New York University's AI Now Institute, which studies the social implications of artificial intelligence. As West explains, ChatGPT is built on more than 60 years of chatbot innovation, starting with the ELIZA program, created at the Massachusetts Institute of Technology in the late 1960s, and including the popular SmarterChild bot on AOL Instant Messenger in the 2000s. West expects this latest version to affect certain industries significantly—but, she says, as uncanny as ChatGPT's emulation of human writing is, it's still capable of only a very small subset of functions previously requiring human intelligence. This isn't to say it represents no meaningful problems, but to West, its future—and the future of artificial intelligence altogether—will be shaped less by the technology itself and more by what humanity does to determine its use.
https://www.thesgnl.com/2023/01/chatgpt-sarah-myers-west/

****

Commerce Secretary Gina Raimondo and Deputy Secretary Don Graves Honor the Life & Legacy of Dr. Martin Luther King Jr.

January 17, 2023

"Everybody can be great because anybody can serve." Martin Luther King Jr.

U.S. Commerce Secretary Gina Raimondo and Deputy Secretary Don Graves participated in service events yesterday in the Washington, D.C. area to honor the life, work, and legacy of Dr. Martin Luther King Jr. MLK Day is the only federal holiday designated as a National Day of Service and honors Dr. King's achievements as a civil rights leader who advocated for equality, justice, and dignity for all.

(*Continued On The Following Page)

Commerce Secretary Gina Raimondo stopped by the Good Success Church to help distribute food to the community. Then, she attended the Missionary Baptist Ministers' Conference to meet with church leaders and honor Dr. King's legacy.

"Today and every day, we honor the life of Dr. Martin Luther King Jr.," said Secretary Raimondo. "As we reflect on his legacy, let us recommit ourselves to his unfinished work. It's up to all of us to continue to fight for equality, stand up to hatred, and improve communities through service."

Deputy Secretary Don Graves joined Secretary of Transportation Pete Buttigieg at Hart Middle School in Washington, D.C. and saw first-hand the incredible work being done by AmericCorps and City Year D.C. to help build strong relationships with students to ensure their success. Graves and Buttigieg joined several volunteers in building a table for the school.

"Martin Luther King Jr. Day is the only federal holiday designated as a National Day of Service," said Deputy Secretary Graves. "Together, we can honor Dr. King's legacy and the work of so many others who stood alongside him to build a more equitable and just America."

Please visit The King Center for more information on the life and legacy of Dr. Martin Luther King, Jr.

****

Insights, analysis and must reads from CNN's Fareed Zakaria and the Global Public Square team, compiled by Global Briefing editor Chris Good

January 20, 2023
Powder-Keg Peninsula

North Korea has posed a nuclear threat for decades. Is it time, again, to worry about it more actively?

Yes, according to a Foreign Affairs essay by Sue Mi Terry, who notes a series of disquieting developments in the last year: a record number of North Korean missile tests; advancements (in smaller, non-intercontinental missiles) in the use of solid fuel, which makes missiles more mobile and faster to launch; and an expansion of North Korea's stated criteria for ordering a preemptive nuclear strike. "Western policymakers and observers are not as concerned as they should be about recent developments," Terry warns. "(T)he security imperative is clear and pressing."

Also disconcerting was a recent suggestion by South Korean President Yoon Suk Yeol that promises of US protection are no longer enough to make South Koreans feel safe. At Foreign Policy, Doug Bandow writes that Yoon was right: "(G)eneric guarantees remain of little value," Bandow writes. "Unless U.S. policymakers are prepared to risk everything for South Korea, they must contemplate the previously unthinkable: a South Korean bomb."

South Korea gaining nuclear weapons is viewed as popular among South Korean citizens, Terry writes in Foreign Affairs; basing US nuclear weapons in South Korea is seen as a goal of the establishment in Seoul, Bandow writes for Foreign Policy. At the Australia-based Lowy Institute's Interpreter blog, Gabriela Bernal sees stakes rising. "North Korea will not take the first step in deescalating tensions," Bernal writes. "This move must come from the South. While it may seem unfair or akin to 'losing face' for Seoul, it is the only way to prevent what could become a catastrophic conflict on the Korean Peninsula."

AUS to buy US-made Black Hawk helicopters

Australia will spend almost $3 billion buying 40 new US-made Black Hawk helicopters for the army, with Defense Minister Richard Marles officially killing off a troubled European project.

****

FOR IMMEDIATE RELEASE
January 18, 2023

Media Contact:
Office of Public Affairs, publicaffairs@doc.gov
Readout of Deputy Secretary Graves' Meeting with Japan's Minister for Internal Affairs and Communications Takeaki Matsumoto

WASHINGTON – Yesterday, Deputy Secretary of Commerce Don Graves met with Japan's Minister for Internal Affairs and Communications Takeaki Matsumoto. The two leaders presided over the signing of a new Memorandum of Cooperation between the National Telecommunications and Information Administration (NTIA) and the Ministry of Internal Affairs and Communications (MIC) on open, resilient telecommunications networks, and reaffirmed the importance of U.S.-Japanese partnership on this shared priority. The meeting also addressed Japan's 2023 G7 presidency, continued support for the development and adoption of Open Radio Access Networks (Open RAN), next steps for efforts in the Quad and the Indo-Pacific Economic Framework for Prosperity, and expanded collaboration between NTIA and MIC.

****

Russia's nuclear entity aids war effort in Ukraine, documents show, leading to calls for sanctions

Rosatom, the state nuclear power conglomerate, has been working to supply the Russian arms industry with components, technology and raw materials for missile fuel, documents show. A letter from a Rosatom department chief, dated from October and obtained by Ukrainian intelligence, shows the company offering to provide goods to Russian military units and to Russian weapons manufacturers that are under sanctions.

****

GLOBAL DEFENSE PURCHASES INCREASE 2022

WASHINGTON — Sales of military weapons between the U.S. and foreign governments shot up to nearly $51.9 billion in fiscal 2022, largely because U.S. allies in Europe are rushing to arm themselves in the wake of Russia's invasion of Ukraine 11 months ago.

The total represented a 49% jump from $34.8 billion in sales the previous year, according to new State Department data. Direct commercial sales — from contractors to governments — also grew, reaching $153.7 billion, up from $103.4 billion the year before.

One factor in the surge is the easing of the global pandemic that in 2021 depressed sales from a spike to $83.5 billion in 2020. Also, since Russia's invasion, European allies and allies in the Pacific have sought U.S. arms to deter Chinese aggression.

One of the biggest orders in 2022 was placed by Indonesia, which analysts see as building a military intended to stave off China. The U.S. approved Indonesia to buy three dozen Boeing-made F-15ID aircraft and related equipment in a deal worth as much as $13.9 billion.

(*Continued On The Following Page)

Japan, Netherlands to Join US in Chip Controls on China

Jenny Leonard

Thu, January 26, 2023 at 10:37 PM EST·

Japan, Netherlands to Join US in Chip Controls on China

(Bloomberg) -- Japan and the Netherlands are poised to join the US in limiting China's access to advanced semiconductor machinery, forging a powerful alliance that will undercut Beijing's ambitions to build its own domestic chip capabilities, according to people familiar with the negotiations.

US, Dutch and Japanese officials are set to conclude talks as soon as Friday US time on a new set of limits to what can be supplied to Chinese companies, the people said, asking not to be named because the talks are private. Negotiations were ongoing as of late Thursday in Washington. There is no plan for a public announcement of restrictions that will likely be just implemented, the people said.

The Netherlands will expand restrictions on ASML Holding NV, which will prevent it from selling at least some of its so-called deep ultraviolet lithography machines, crucial to making some types of advanced chips and without which attempts to set up production lines may be impossible. Japan will set similar limits on Nikon Corp.

A spokeswoman for the National Security Council declined to comment.

The joint effort expands on restrictions the Biden administration unveiled in October that were aimed at curtailing China's ability to manufacture its own advanced semiconductors or buy cutting-edge chips from abroad that would aid military and artificial-intelligence capabilities. The three countries are home to the most important companies that produce equipment for manufacturing chips, including ASML, Japan's Tokyo Electron Ltd. and the US's Applied Materials Inc.

https://finance.yahoo.com/news/japan-netherlands-join-us-chip-014759438.html

****

Russian tech tycoon heads to trial over insider trading hacking scheme

By Shelley Murphy Globe Staff, Updated January 27, 2023, 7:12 p.m.
Vladislav Klyushin portrayed himself as an up by-the-bootstraps businessman, who grew up poor, has been working since he was 13 years old, and built a profitable information technology company that employs more than 100 people. He has a law degree, previously worked as a professor at the Moscow State Linguistic University, and was awarded a Medal of Honor by Russian President VladimirPutin several years ago.

But behind that facade, federal prosecutors in Boston allege, the 42-year-old millionaire orchestrated an elaborate global hacking and insider trading scheme. They say he conspired with four codefendants — including a former Russian military intelligence officer who served as deputy director of Klyushin's company and was previously charged with interfering in the 2016 US presidential election — to hack into the servers of two vendors that publicly traded companies use to make filings to the Securities and Exchange Commission.

*(*Continued On The Next Column)*

Between 2018 and 2020, prosecutors allege, Klyushin and his co-conspirators viewed the earnings reports of dozens of companies — including Tesla, Hubspot, Datadog, and Snap — before they were made public, and used that information to make stock trades that led to millions of dollars in illegal profits.

"This is sort of like insider trading on steroids," said attorney Robert Fisher, a former federal prosecutor, adding that insider trading cases generally involve information related to one company or a sliver of an industry. Hacking into a vendor with access to multiple companies is rarer and much more lucrative, he said; an SEC complaint filed in federal court in Boston alleges the conspirators raked in $82.5 million. Now, Klyushin, a married father of five, is set to go to trial Monday in federal court in Boston on charges of conspiracy, wire fraud, unauthorized access to computers, and securities fraud, in a case that will be closely watched in diplomatic circles in the United States and Russia, according to legal experts. Klyushin owns a Moscow-based technology company, M-13, that provides media monitoring and cybersecurity testing for private and public entities, including the Russian Federation, and has "significant ties to the Russian government, and, more specifically, to parts of the Russian government engaged in defense and counter-espionage," prosecutors said in court filings.

In response to defense concerns about whether Klyushin will receive a fair trial, US District Judge Patti B. Saris has agreed to question potential jurors about whether they feel any bias toward Russian nationals, but rejected a request to ask them about their feelings on the war in Ukraine. She also ruled that prosecutors may not mention Putin's name during the trial.

Klyushin was first arrested in March 2021 after he arrived via a chartered jet in Switzerland, where a helicopter was waiting on the tarmac to whisk him and his family to a nearby luxury ski resort for a planned vacation. Local police swooped in at the request of US authorities. His codefendants were in Russia, a country with no extradition treaty with the United States; Swiss authorities extradited Klyushin to the United States nine months later, rejecting the Russian government's request to send him home instead.

Last year, Klyushin's name surfaced as part of a potential prisoner swap for American basketball star Brittany Griner and former US Marine Paul Whelan. Though Griner was released in December in exchange for convicted Russian arms dealer Viktor Bout, Whelan remains imprisoned in Russia, serving a 16-year sentence for espionage. Whelan says he's innocent and was framed, but he dropped his appeal as his supporters continue to pressure the Biden administration to secure his release.

Meanwhile, Klyushin has been held without bail at the Plymouth County jail since his extradition 13 months ago. A federal judge refused to set bail, saying he's a serious risk of flight. He owns property in London and Russia and has access to private planes, helicopters, and a 77-foot yacht he purchased for nearly $4 million. Prosecutors say he faces more than 20 years in prison if convicted.

"It wouldn't be surprising to find that the Russians are trying to trade for him," said Jamil Jaffer, executive director of the National Security Institute at George Mason University's Antonin Scalia Law school. He noted that one of Klyushin's codefendants is Ivan Ermakov, who was charged with interfering with the 2016 US election. "They obviously don't want information coming out about his association with a known Russian intelligence officer who turns out to be the deputy director of his company."

*(*Continued On The Following Page)*

The US attorney's office declined to comment on Klyushin's case or whether he is being eyed for a prisoner swap. Attorney Maksim Nemtsev, who represents Klyushin, also declined to comment.

Fisher, who was a senior litigation counsel at the Financial Industry Regulatory Authority before becoming a partner at Nixon Peabody, said such cases are complex and can be difficult to prove because hackers "thrive on anonymity," and it may be challenging to link a particular hacker to an intrusion, especially when they are located in a foreign country that doesn't cooperate with US investigators.

Klyushin's lawyers wrote in court filings that they will offer "substantial challenges" to the government's case and argued that a preliminary review showed he actually lost $3.6 million on transactions involving Tesla stock during the period that prosecutors allege he had inside information.

"Such staggering losses are inconsistent with the government's theory of Mr. Klyushin having advanced knowledge of material non-public stock information," Klyushin's lawyers wrote in a December 2021 memorandum arguing unsuccessfully for his release on bail.

The defense lawyers successfully petitioned the judge in the case to bar the government from presenting evidence that Klyushin's fugitive codefendant was a former Russian military intelligence officer and was indicted in 2018 in Washington, D.C., and Pennsylvania for two alleged computer hacking schemes, involving the 2016 election and one that allegedly targeted anti-doping agencies and officials.

Klyushin's attorneys argued in court filings that the government's case is "entirely circumstantial" and the charges are unfounded.

Boston attorney B. Stephanie Siegmann, a former federal prosecutor who handled a case against an Iranian national that was dismissed by the Obama administration in 2016 as part of a sweeping nuclear deal involving prisoner swaps, said line prosecutors have no say in whether a defendant will be freed as part of an international trade.

"That's a diplomatic, political decision," Siegmann said.

But Klyushin's case will be "closely watched" in Russia because he was charged with someone "who was clearly working with the Russian government in the election disinformation campaign," said Siegmann, speculating that Russia may try to negotiate Klyushin's release if he is convicted and sentenced to prison.

Computer hacking and insider trading cases have become a priority for the Justice Department over the past decade, and the case against Klyushin is significant because of the scope of the scheme and his political ties, she said.

"There's a lot of hacking that is done by the Russians and Ukrainians and there are a lot of criminal organizations involved in that activity in those countries, doing it to make money," said Siegmann, a partner at Hinckley Allen, where she chairs the law firm's International Trade & Global Security group. But, she added that it can be difficult to bring a Russian national to trial in the United States because there is no extradition treaty between the two countries.

In Klyushin's case, US authorities learned about his planned ski trip and moved quickly. A day before his arrival in Switzerland, federal prosecutors filed the criminal charges in Boston under seal and secretly obtained a warrant for his arrest.

Microsoft Teams Outage Affects Millions Around the World

By James Bickerton On 1/25/23 at 3:43 AM EST

Users around the world are reporting Microsoft Teams, the communications platform used by many businesses, has stopped working.

Faults have also been reported on email service Microsoft Outlook, as well as a number of other products owned by Microsoft.

In an update posted on Twitter, Microsoft said: "We're investigating issues impacting multiple Microsoft 365 services. More info can be found in the admin center under MO502273."

We're investigating issues impacting multiple Microsoft 365 services. More info can be found in the admin center under MO502273.

— Microsoft 365 Status (@MSFT365Status) January 25, 2023

Microsoft later added: "We've identified a potential networking issue and are reviewing telemetry to determine the next troubleshooting steps."

We're investigating issues impacting multiple Microsoft 365 services. More info can be found in the admin center under MO502273.

— Microsoft 365 Status (@MSFT365Status) January 25, 2023

Azure, Microsoft's cloud unit, also reported problems, tweeting: "We are currently investigating a networking issue impacting connectivity to Azure for a subset of users. More information will be provided as it becomes available."

According to website Down Detector, which monitors the performance of major online platforms, a flood of reports claiming Teams wasn't working began to come in around 6:59 a.m. GMT (1:59 a.m. ET).

At 6:44 a.m. GMT the website hadn't received a single new report of the service not working, but this surged to 219 at 7:12 a.m. GMT, followed by a high of 279 at 7:44 a.m. GMT.

In the Down Detector comment section users from all over the world discussed the problems they were having with Teams in their respective countries.

One user wrote: "MS Teams suddenly stops working. Manila."
Another posted: "No screen sharing and chat, audio is sketchy – Poland."

A third said: "Both Denmark and the Philippines have huge issues, we can attend meetings and talk, but not share screens, and hardly video."

Former FBI official arrested, faces charges of violating Russian sanctions

Jan. 23, 2023,
By Jonathan Dienst and Tom Winter

Federal prosecutors say the former head of counterintelligence for the FBI's New York office laundered money, violated sanctions against Russia while working with a Russian oligarch and while still at the FBI took hundreds of thousands of dollars from a foreign national and former foreign intelligence official.

Charles McGonigal, 55, was arrested on Saturday after arriving at JFK airport in New York on a flight from the Middle East.

A case filed in federal court in Washington, D.C., alleges that while serving as Special Agent in Charge of FBI counterintelligence efforts in the New York office, McGonigal took $225,000 in cash from an individual with business interests in Europe who had been an employee of a foreign intelligence service.

From August 2017 through his retirement in September 2018, McGonigal allegedly concealed his relationship with this former foreign security officer from the FBI. He allegedly requested and received cash from the individual and traveled abroad with the individual.

"Mr. McGonigal betrayed his solemn oath to the United States in exchange for personal gain and at the expense of our national security," said FBI Assistant Director in Charge Donald Alway.

Federal prosecutors in New York allege that after his 2018 retirement from the FBI, McGonigal worked with Russian oligarch Oleg Deripaska, Deripaska associate Sergey Shestakov, and a third person to investigate a rival Russian oligarch in return for payments from Deripaska.

According to prosecutors, McGonigal, Shestakov and the third person tried to conceal Deripaska's involvement through shell companies, forged signatures and other means.

U.S. Attorney for the Southern District of New York Damian Williams said, "As alleged, Charles McGonigal, a former high-level FBI official, and Sergey Shestakov, a Court interpreter, violated U.S. sanctions by agreeing to provide services to Oleg Deripaska, a sanctioned Russian oligarch. They both previously worked with Deripaska to attempt to have his sanctions removed, and, as public servants, they should have known better."

FBI Assistant Director in Charge Michael J. Driscoll said, "The FBI is committed to the enforcement of economic sanctions designed to protect the United States and our allies, especially against hostile activities of a foreign government and its actors. Russian oligarchs like Oleg Deripaska perform global malign influence on behalf of the Kremlin and are associated with acts of bribery, extortion, and violence."

The Treasury Department has sanctioned Deripaska for "having acted or purported to act on behalf of, directly or indirectly, a senior official of the Government of the Russian Federation and for operating in the energy sector of the Russian Federation economy," according to the Justice Department. In 2022, federal prosecutors in New York charged Deripaska with violating sanctions.

*(*Continued On The Following Column)*

Given McGonigal's ties to the Washington and New York area offices of the FBI, the Los Angeles field office led the two-year-long investigation, three senior law enforcement officials said. The decision to move the probe to Los Angeles was to ensure there were no conflicts of interest or competing interests among agents who may have known McGonigal.

McGonigal's career included a stop as a section chief coordinating the FBI's cyber and counterintelligence programs at the FBI's secretive Intelligence Technology and Data Division (ITADD) in Chantilly, Virginia, as well as his position in New York, public records show.
McGonigal was named special agent in charge of the Counterintelligence Division for the New York Field Office in 2016, after serving as the section chief of the Cyber-Counterintelligence Coordination Section at FBI headquarters.

McGonigal joined the FBI in 1996, and was first assigned to the New York Field Office, where he worked on Russian foreign counterintelligence and organized crime.

During his tenure in New York, he worked on the TWA Flight 800 investigation, was assigned to the task force investigating scientist Wen Ho Lee, investigated the 1998 terrorist bombings of the U.S. Embassies in Tanzania and Kenya, and investigated the Sept. 11, 2001, terror attacks.

Seth DuCharme, McGonigal's attorney, said, "Charlie served the U.S. effectively for decades. He will plead not guilty. We look forward to seeing the evidence."

DuCharme said he expected McGonigal to be released from custody Monday.

****

Defendant Admits Using Intermediary to Funnel Payments for United States Army Aviation-Related Software Sent to Restricted Beijing University

SAN FRANCISCO – Jonathan Yet Wing Soong pleaded guilty today to violating export control laws in connection with a scheme to secretly funnel sensitive aeronautics software to a Beijing university, announced United States Attorney Stephanie M. Hinds; Federal Bureau of Investigation Special Agent in Charge Robert K. Tripp; Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement (BIS), Special Agent in Charge John D. Masters; Defense Criminal Investigative Service (DCIS) Special Agent in Charge Bryan D. Denny. The plea was accepted by the Hon. Susan Illston, United States District Judge.

Between August 2016 and September 2020, Soong, 35, of Castro Valley, Calif., was employed as a program administrator by Universities Space Research Association (USRA), a nonprofit research corporation focusing on advancing space science and technology. In April of 2016, USRA contracted with the National Aeronautics and Space Administration (NASA) to, among other things, license and distribute aeronautics-related Army flight control software for a fee. Soong's duties included, among other things, conducting and servicing software license sales, conducting export compliance screening of customers, generating software licenses, and exporting software pursuant to purchased licenses.

*(*Continued On The Following Page)*

As part of his duties, Soong was responsible for vetting customers to ensure they did not appear on certain restrictive lists—including the Department of Commerce's Entity List and other U.S. government lists—that placed limitations on the transfer of products to identified entities. In pleading guilty, Soong admitted that he willingly exported and facilitated the sale and transfer of restricted software to Beihang University knowing that the university was on the Department of Commerce's Entity List. According to government filings in the case, Beihang University was added to the Entity List due to the University's involvement in People's Republic of China military rocket systems and unmanned air vehicle systems. In his plea agreement, Soong acknowledged he used an intermediary to complete the export of the program to avoid detection that the real purchaser was on the Entity List.

At issue in the case is a software package referred to as CIFER, a tool that allows a user to develop a dynamic model of an aircraft, based on collective flight test data using system identification techniques. According to government filings, the package could be used to analyze and design aircraft control systems. According to his plea agreement, Soong was aware in April of 2017 that the CIFER software was subject to Export Administration Regulations and that Beihang University was on the Entity List thus making it necessary to obtain a license prior to exporting the CIFER software to the university. Soong acknowledged that he nonetheless arranged to sell and transfer the CIFER software package to the entity without obtaining a license.

The plea agreement describes how, on May 1, 2017, a representative of the university communicated with Soong and expressed an interest in exploring an arrangement in which rather than use Beihang University as the purchaser of the CIFER software, the purchase would be made in the name of a third-party small company. For the next several months, Soong communicated with the representative and then, in late 2017, Soong communicated with a representative from Beijing Rainbow Technical Development Ltd. (Beijing Rainbow), identified as being the third-party intermediary for the sale of the CIFER software to Beihang University. Soong ultimately exported directly to Beihang University. In July 2018, Soong also arranged to have the passcodes for the CIFER software package forwarded to Beihang University with payment coming from Beijing Rainbow.

On September 26, 2022, Soong was charged by information with one count of violating the International Emergency Economic Powers Act (IEEPA), in violation of 50 U.S.C. §§ 1702 and 1705. Pursuant to today's agreement, Soong pleaded guilty to the count.

The IEEPA violation carries a statutory maximum penalty of 20 years in prison and a $1,000,000 fine. In addition, as part of any sentence, the court may order restitution and up to three years of supervised release. However, any sentence after conviction will be imposed by the court only after consideration of the U.S. Sentencing Guidelines and the federal statute governing the imposition of a sentence, 18 U.S.C. § 3553.

Soong remains out of custody pending sentencing. Judge Illston scheduled Soong's sentencing hearing for April 28, 2023. Assistant United States Attorney Barbara Valliere of the United States Attorney's Office's Special Prosecutions Section is prosecuting the case with the assistance of Maddi Wachs and Kathy Tat. The prosecution is the result of an investigation by the BIS, DCIS, and the FBI with assistance from the NASA Office of Inspector General; U.S. Army Criminal Investigation Division; the U.S. Army Counterintelligence; and the Department of Homeland Security, Homeland Security Investigations.

Updated January 17, 2023

WHAT TO DO WHEN OSHA SHOWS UP
By: Darcy Cook, Safety Trainer

We have been providing safety support and services for over 20 years and we have never had 6OSHA citation cases open at the same time. We usually do 3-4 a year. Additionally, we have never mediated a Targeted Industries Citation. Why? My guess, OSHA never had enough staff to get to targeted industry inspections and now they do.

I recently attended an OSHA webinar hosted by OSHA enforcement and educational providers. They opened the webinar announcing that they were hiring and that jobs working for OSHA are available.

Since the day before Thanksgiving, our inbox has been filled with companies who have had a visit from OSHA. Currently, we have 6 businesses who have reached out because OSHA showed up on their front door.

Industry	Description	Location
Construction Site	Incident Fall Protection	Massachusetts
Public School System	Incident HazCom	Massachusetts
Residential Construction	Incident Fall Protection	Massachusetts
Manufacturing	Targeted Emphasis Program for Amputations	Massachusetts
Manufacturing	Targeted Emphasis Program for Amputations	Rhode Island
Trucking Company	Employee Complaint Power Industrial Trucks	Rhode Island

If OSHA showed up, would you know what to do? When you don't know what to do, it makes our jobs harder. Here are the tips and the process of an investigation. Learn the process, put a plan in place to manage or respond to it.

1. The agent will announce themselves and present credentials
2. Place them in an isolated conference room without walking them through your production areas.
3. Get the right people in the room for the opening conference. Here is where they will explain to you why they are there.
4. Do not provide information to them on topics that do NOT relate to the reason they are there. Do not give them a tour of the entire facility. Only show them what they are asking to see. Limit and control their exposure.
5. They will ask for documents to include training records, policy, procedures, checklists, and inspections. Only bring them what they ask for and related to the topic.
6. They will ask to see certain parts of your operation. Stay with them. Control the paths you take and what the employees are doing. This might be a good time for employees to take a break.
7. If they take a photograph, you should too. If they take a video, you should too.
8. If they show you a violation and give you the opportunity to fix it, do it immediately
9. They will potentially ask to interview your staff. Give them an isolated area to do so.
10. They will do a closing conference where they will describe to you what potential citations you will receive, write them all down.
11. Teach your front desk/receptionist, what to do, who to call and where to place the OSHA agent.
12. If you have a relationship with a safety consultant, call them immediately while OSHA is there.
13. Once OSHA leaves, you pretty much know what they are concerned with, so get to work fixing everything immediately and get your training up to date, if applicable.

You will have approximately 21 days before you see the citation letter. Citations are not issued immediately following the inspection. They report is written and reviewed by the Area Director before presenting to you. Once you receive the letter, you have 15 days to respond.

(*Continued On The Following Page)

1. Litigate and fight the citation
2. Pay it
3. Ask for an Informal Conference

We strongly encourage you to ask for an informal conference and show them all of the changes and trainings completed to date. If you are not a repeat offender, you will get some "goodwill" in the final decision of your citations and penalties.

We strongly recommend that you get the support and assistance by professionals and providers who have gone through this process.
OSHA has a consultation division that is of no cost to you. Just be advised, you will need to fix everything they identify as a non-conformance and safety hazard.

To learn more about what to expect during an OSHA inspection go to OSHA.gov and/or find a safety consultant [or just contact us. Safety Trainers info@safetytrainers.com]

****

Press Release

The U.S. Department of Commerce Announces Two Stakeholder Listening Sessions for the IPEF Special Negotiating Round
01/19/2023 09:38 AM EST

Office of Public Affairs
publicaffairs@doc.gov

The U.S. Department of Commerce invites interested stakeholders to participate in a stakeholder listening session opportunity on February 1, 2023, in advance of the special negotiating round for Pillars II-IV of the Indo-Pacific Economic Framework for Prosperity (IPEF) in New Delhi, India.

In addition, the Government of India is organizing two in-person stakeholder events in New Delhi for the IPEF special negotiating round. Stakeholders interested in participating in one or both events should register per the instructions below.

The special negotiating round hosted by the Government of India in New Delhi will be for IPEF Pillar II (supply chains), Pillar III (clean economy), and Pillar IV (fair economy).

All stakeholder events are closed to the press.
DEPARTMENT OF COMMERCE LISTENING SESSION
Event Details

Date: Wednesday, February 1, 2023
Time: 9:00am – 10:30am (Eastern Time)
Venue: Virtual

Registration

Registration for ***all participants*** must be sent to USCommerceIPEF@trade.gov. In the email, please use the subject line "Department of Commerce IPEF Listening Session." Registration will close at **12:00pm (Eastern Time) on Tuesday, January 31, 2023.** Please indicate whether you are interested in providing a short intervention or presentation at the event. The time permitted for presentations will depend on the number of confirmed stakeholder presenters.

(*Continued On The Following Column)

NEW DELHI STAKEHOLDER EVENTS
Event Details

Date: Thursday, February 9, 2023
Time: 2:00pm-5:00pm (India Standard Time) for a stakeholder listening session

Time: 6:00pm-7:00pm (India Standard Time) for a stakeholder reception

Venue: New Delhi, India

Registration

Interested participants should email USCommerceIPEF@trade.gov to receive the registration information package. In the email, please use the subject line "New Delhi Stakeholder Registration." **Registration will close at 12:00pm (Eastern Time) on Friday, January 27, 2023.** Participants will have the option to provide a short intervention or presentation at the stakeholder listening session. Participants can participate in one or both of the New Delhi stakeholder events and should note which events they are interested in when contacting USCommerceIPEF@trade.gov for the registration information and additional details.

Additional information on the Indo-Pacific Economic Framework for Prosperity:

In May 2022, the United States launched the Indo-Pacific Economic Framework for Prosperity (IPEF) with Australia, Brunei Darussalam, Fiji, India, Indonesia, Japan, the Republic of Korea, Malaysia, New Zealand, Philippines, Singapore, Thailand, and Vietnam. The IPEF will advance resilience, sustainability, inclusiveness, economic growth, fairness, and competitiveness for our economies. The 14 IPEF partners represent 40 percent of global GDP and 28 percent of global goods and services trade.
The IPEF features four pillars: (I) Trade; (II) Supply Chains; (III) Clean Economy; and (IV) Fair Economy. On September 9, 2022, the United States and IPEF partners issued ministerial statements outlining the scope of future negotiations for the Pillars of the IPEF.
Beginning on February 8, 2023, the Department of Commerce, along with interagency colleagues, will join the IPEF partners for the IPEF special negotiating round in New Delhi, India.

****

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

Remarks as Prepared for Delivery by Assistant Secretary for Export Enforcement Matthew S. Axelrod to the 12th Annual Forum on U.S. Export & Re-export Compliance for Canadian Operations

January 31, 2023

Thank you for the introduction.
It's great to be with you here in Toronto as you kick off the 12th Annual Forum on U.S. Export and Re-export Compliance for Canadian Operations. I'm particularly grateful to have the opportunity to speak with you this morning about how the United States and Canada are continuing to strengthen our export enforcement partnership.

(*Continued On The Following Page)

Canada and the United States share more than just a border. We share a common perspective. We're partners in the collective effort to create a safe, secure, and prosperous North America. Our economies are deeply integrated, and we enjoy the largest bilateral trade and investment relationship in the world. The almost 400,000 people and $2.6 billion worth of goods and services that cross our shared border every day are a testament to the strength of our economic relationship. We're also enforcement partners. Our two governments work together closely to bolster our shared continental security against domestic, regional, and global threats. President Biden and Prime Minister Trudeau reaffirmed this shared commitment at the North American Leaders' Summit earlier this month. As you'll hear shortly, within our countries' general law enforcement partnership, we have established a specific and impactful relationship on export enforcement. But first, a quick story about the Ukrainian men's ice hockey team.

This month, the United States and Canada – along with 48 other countries from around the world – competed in the 2023 Winter World University Games in Lake Placid, New York. Staged every two years in a different city, the winter edition of the World University Games is the largest multi-sport winter event in the world, after the Winter Olympics. The Games combine high-level competitive sport – from ice hockey to snowboarding – with educational and cultural events. As the largest gathering of college athletes on the planet, the Games provide a unique opportunity for students to represent their respective countries and connect with other students from around the globe.

But the real story of this year's Winter Games is one not of competition, but of cooperation.

Since Russia further invaded Ukraine last February, Ukrainians have celebrated major victories – like breaking the siege of Kyiv – and have endured major destruction, like the bombardment of Bakhmut. They have dealt with constant missile strikes, power outages, and a lack of basic necessities. Yet, somehow, in the middle of a war, despite the incredible hardship, the Ukrainian under-25 men's hockey team has managed to persevere.
The Canadian Hockey Federation and other Canadian sponsors made it possible for the team to come and tour Canada prior to the Winter Games. The Ukrainians played exhibition games against Canadian universities to raise money for humanitarian causes in Ukraine. Once at the Games themselves, they beat Sweden in a decisive 12-2 victory. Following the victory, Ukrainian Defenseman Arsen Paliichuk told a reporter: "We were motivated to win this game so the people back home could have some kind of hope and something to believe in over there." Without Canada's support, none of this would have been possible. The Ukrainian hockey team likely never would have even made it to the Games.

It is this hybrid of competition and cooperation, of representing one's own country's interests but also being part of something larger and interconnected, that I want to speak about with you today.

Simply put, export controls are a shared endeavor. And when it comes to export enforcement, cooperation is critical to ensure our shared security.

At the U.S. Department of Commerce, where I am the Assistant Secretary for Export Enforcement, our team of law enforcement agents and analysts is focused on a singularly important mission: keeping our country's most sensitive technologies out of the world's most dangerous hands.

(*Continued On The Following Page)

At no point in history has this mission been more important, and at no point have export controls been more central to our collective security, than right now. Countries implementing multilateral export control regimes have long known that such controls are critical to the world's safety, and most effective when widely implemented across the globe. But our current geopolitical challenges, the increasingly rapid development of technology with the potential to provide asymmetric military advantage, and the countless ways in which the world is now interconnected, have raised the prominence and impact of export controls in unprecedented ways.

And that means that the importance of export enforcement has risen in unprecedented ways as well. It's not sufficient for likeminded countries just to have parallel controls on paper. It's critically important, but it's not sufficient. We also need to ensure a common commitment to effective implementation and enforcement of those controls.

In other words, export enforcement must be a shared focus across the globe. Strong multilateral export enforcement coordination is essential to keeping the world safe. All likeminded countries should be looking to build their export enforcement capacity, both individually and collectively. That enforcement capacity will help protect countries' own sensitive goods and technologies – as well as those of their allies – from being transferred to countries or entities that may use them for harmful purposes such as destabilizing military modernization, proliferation of weapons of mass destruction, support for terrorism, or human rights abuses.

There are, of course, challenges to ensuring effective export control enforcement. For example, enforcement responsibility resides in different agencies in different countries, but often is handled as part of a country's Customs bureau. Customs bureaus, understandably, are often preoccupied with preventing harmful items – like drugs and weapons – from coming into a country and therefore are sometimes less focused on sensitive items – like technologies that can be used to support military modernization programs – from going outbound.

But given the increase in security risk that advanced technologies – such as quantum computing, hypersonic weapons, and unmanned aerial vehicles – now pose, we need all likeminded countries to invest in their export enforcement capacity. Unlike other geopolitical challenges, export enforcement cannot be effective unless there is a coordinated global effort. Without such an effort, bad actors can simply bypass one country's controls and source a sensitive commodity elsewhere. It's only by working together, with strong enforcement regimes across countries, that we can truly protect technologies that need protecting.

We've done this before. Up until 1977, when the United States passed the Foreign Corrupt Practices Act (FCPA), no country in the world considered the bribing of foreign officials for business purposes to be illegal. Twenty years later, the Organization for Economic Cooperation and Development's (OECD) Anti-Bribery Convention was signed. The Convention – eventually ratified by 44 countries, including the United States and Canada – illustrates a shared global understanding of the importance of combating bribery of foreign public officials. In other words, the world shifted. Countries took collective action against a common challenge and built a multilateral enforcement coordination mechanism to combat foreign corrupt practices.

(*Continued On The Following Page)

We're now beginning to see that same shift with respect to export enforcement. As our country's Deputy Attorney General, Lisa Monaco, stated last year, export and sanctions enforcement are "the new FCPA." In other words, just as the U.S. Department of Justice previously ramped up enforcement of its foreign bribery statute and worked with partners around the world to ensure a robust global enforcement focus, so too is the United States now ramping up sanctions and export control enforcement. Like bribing a foreign official, exporting the most sensitive goods and technologies without appropriate safeguards is a collective harm; and we must work collectively as partners – through coordinated and aggressive enforcement action – to prevent these sensitive goods and technologies from falling into the wrong hands.

The events of the past year provide a stark example of the increasing importance of international export enforcement capacity and coordination. After Russia launched its brutal and unprovoked war against Ukraine last February, 38 countries – including the United States and Canada – coalesced to put in place the most expansive export controls in history aimed at a specific country. Both my colleagues at BIS Export Administration and their counterparts at Global Affairs Canada deserve immense credit for enacting these unprecedented – and based on Russia's responses – increasingly stringent export controls.

The controls are working to degrade Russia's ability to wage its unjust war against Ukraine. Global exports of semiconductors to Russia, for example, have seen a sustained decline of approximately 70 percent since the invasion began, leaving Russian companies without the chips they need for weapons like precision guided missiles and tanks. The Russian defense industry has struggled to replace weapons destroyed in the war, including over 6,000 pieces of military equipment, such as armored personnel carriers and infantry fighting vehicles. Russian hypersonic ballistic missile production has virtually ceased due to the lack of necessary equipment.

But it's not enough just to impose multilateral controls; to be effective, controls need to be aggressively enforced, not only by the United States but through coordinated work with coalition partners. For the United States and Canada, that means coordinated work by our respective enforcement teams – my Export Enforcement team at the Bureau of Industry of Security (BIS) and Canada Border Services Agency (CBSA) here in Canada.

CBSA and BIS have enjoyed a successful relationship over the past decade, but the events of February 24, and the resulting export control rules, required intensified collaboration. And so, last June, BIS and CBSA announced a joint commitment to leverage our authorities and resources to detect, deter, and stop export violations.

Our first step in this process was to initiate quarterly senior-level meetings between our teams, where we strategize on how best to leverage our combined resources to enforce our complementary export control rules. In fact, this is precisely the reason I am in Canada this week – to meet with CBSA, as well as our colleagues from GAC and the Royal Canadian Mounted Police (RCMP), where we will: share information on diversion actors; coordinate the targeting and conduct of pre- and post-shipment verifications and audits; upgrade joint efforts to inspect, detain, and seize illicit shipments; and work to reduce threats through coordinated outreach, investigations, and enforcement actions.

(*Continued On The Following Column)

Our second step was to establish a BIS enforcement analyst position in Ottawa to liaise on export controls directly and daily with CBSA and our other Canadian partners like GAC and RCMP. Since last summer, we've had an analyst stationed in Ottawa on a rotating basis. We are now in the process of hiring someone to fill a dedicated position there. This will be the first time ever that BIS has embedded a full-time analyst outside of the United States.

This partnership is already bearing fruit. During one of the temporary deployments last year, BIS and CBSA's Counter Proliferation Operations Section (CPOS), working with U.S. Customs and Border Protection, stopped a shipment of drone antennas on the tarmac in Alaska before they could be illegally exported. Drone antennas are used to either transmit or receive electrical signals and, in layman's terms, tell the drone where to go and what to do when it gets there. This interdiction is just one example of "intelligence to action" – a term used by our colleagues at CBSA to illustrate how we use real-time intelligence to take action and stop illicit procurement efforts.

And just today, we placed onto our Entity List seven Iranian unmanned aerial vehicle producers for providing drones to Russia that are being used to attack civilian infrastructure in Ukraine. As many of you are aware, Canada's export control regulations have restricted U.S.-origin goods destined to Iran since 1997, meaning that diverters can't circumvent our regulations by transshipping through Canada or vice versa. Given the threat posed by Iran's support for Russia's war machine, our increasingly close bilateral relationship on export enforcement –including our placement of an analyst in Ottawa – better positions us to prevent U.S. and Canadian technologies from enabling Iran's UAV program.

Collaboration on enforcement doesn't stop with just us and Canada. We are also working to coordinate more broadly with our other Five Eyes partners, as well as with ASEAN countries like Singapore, Malaysia, and the Philippines. And just last month, the U.S.-EU Trade and Technology Council (TTC) reaffirmed the importance of enforcing export controls in a parallel manner. The TTC resolved to take "additional steps to enhance enforcement collaboration between the United States and the European Union, including through the exchange of best practices . . . and with a view to promoting the consistent application of sanction-related export restrictions targeting Russia and Belarus." The EU and the U.S. have since piloted an information exchange on Russian diversion tactics and are actively planning exchanges of best practices, building upon the successes of our partnership with CBSA and GAC.

While 2022 required intense work on Russia, Russia was not our only priority. We remain laser-focused on the risk posed by other nation-states, such as the People's Republic of China (PRC), Iran, and North Korea.

To give a recent example of the challenges we face, just two weeks ago, a California man pled guilty for violating export control laws by secretly funneling sensitive aeronautics software to a Beijing university. The recipient, Beihang University, had previously been placed on our Entity List for helping to develop the PRC's military rocket systems and unmanned air vehicle systems.

This case helps illustrate how the domains of national security and of academia are growing increasingly interconnected. To address this dynamic, we are actively engaging with U.S. academic institutions and research centers, in part through our Academic Outreach Initiative, on ways they can help safeguard their advanced research. We're also working closely with our Canadian counterparts in helping academic institutions protect themselves from current and future threat actors.

(*Continued On The Following Page)

We also changed our policy on how we respond to a host government that is preventing our ability to conduct end-use checks overseas. We've found that the governments of foreign countries, like Canada, generally welcome our end-use checks, as they are eager to support their companies in receiving U.S. exports and participating freely in the global economy. When a foreign government prevents our attempts to conduct an end-use check for a sustained period, however, we are faced with the unacceptable risk that U.S.-origin goods or technology will be misused, given our inability to verify a company's compliance with our controls. Under our new policy, such governments now have a choice. If they cooperate and the end-use checks are successful, then companies will be removed from our Unverified List. On the other hand, if they continue to prevent our end-use checks, we will initiate the process to have companies added to our Entity List.

This new policy is having real world impact. After the policy became effective, we were able to complete successful end-use checks in China for the first time in over two years. In December, we removed 25 Chinese entities from our Unverified List after the satisfactory completion of end-use checks and verification of those entities' bona fides in cooperation. And the policy has had an impact in other ways as well. We didn't only remove entities from our Unverified List in December – we also moved nine Russian companies onto the Entity List because of Russia's sustained failure to schedule our end-use checks.

End-use checks provide us with unique insight into the reliability of foreign parties around the globe, insight that we can then share with our partners like GAC and CBSA to inform their licensing and enforcement decisions. As a result, when we expand our Export Control Officer (ECO) footprint abroad, it has direct implications for safeguarding not only U.S. exports, but also Canadian ones. Right now, we have ECO positions located in seven places around the world, in Beijing, Hong Kong, Frankfurt, Singapore, Istanbul, New Delhi, and Dubai. I'm excited to share that we're now adding two more ECO positions, one in Helsinki and the other in Taiwan. These new positions, plus our new Export Control Analyst position in Ottawa and our enhanced partnership arrangement with CBSA, mean that we now have more resources devoted to protecting U.S. and Canadian technology from diversion than ever before.

I'll close with this. There's a quote from a prominent Canadian that has been repeated so often it is now a cliché. I'm sure you've heard it as something Wayne Gretzky said: "Skate to where the puck is going to be, not to where it has been." The quote captures the idea that we need to anticipate events and get ahead of them, lest we fall behind. That sentiment is most assuredly true for export enforcement. In our rapidly changing world, export controls are critical to protecting our collective global security. That's why we need all likeminded countries to build up their enforcement capacity, as well as to coordinate their enforcement efforts multilaterally. That's where we need to skate, because that's where the puck is going.

While I imagine you've heard the quote before, two things about the quote you may not know. First, it's not actually a Wayne Gretzky quote. It's a quote from Wayne's father, Walter Gretzky. And, second, it wasn't just an exhortation. It was a method of training. Walter Gretzky had his young son Wayne watch hockey games on television and trace the movement of the puck on a piece of paper. When the game was done, Wayne had essentially created a map – a record of where the puck had spent the most time and where it had spent the least. After tracing hundreds of games this way, Wayne Gretzky learned to anticipate where the puck was going instinctively – not because of innate genetic talent, and not because of his father's mere words, but because he put in the hard work, day after day after day, of methodically building his capacity.

Just as the last few decades have seen the expansion of multilateral antibribery enforcement, I am confident the next few will include a worldwide movement to combat export violations. But that movement won't happen by itself. It is going to take sustained effort, by all of us, day after day after day, to build up our individual – and collective – enforcement capacity.

It's been 34 years to the month that the first free trade agreement between the United States and Canada entered into force, and our relationship is stronger than ever. As President Biden said while announcing the U.S.-Canada Partnership Roadmap two years ago, we share a unique bond as friends, neighbors, NATO Allies, and partners. I look forward to continuing to strengthen that bond in the months and years ahead.

NEW FINE RATES

Summary

Citation in 22 CFR	FY22 Max penalties	New (FY 23) max penalties
§ 35.3	$12,537 up to $376,138	$13,508 up to $405,270.
§ 103.6(a)(1) *Prohibited Acts*	$42,163	$45,429.
§ 103.6(a)(2) *Recordkeeping Violations*	$8,433	$9,086.
§ 127.10(a)(1)(i)	$1,272,251	the greater of $1,200,000 or the amount that is twice the value of the transaction that is the basis of the violation with respect to which the penalty is imposed.
§ 127.10(a)(1)(ii)	$925,041 or five times the amount of the prohibited payment, whichever is greater	$996,685, or five times the amount of the prohibited payment, whichever is greater.
§ 127.10(a)(1)(iii)	$1,101,061	$1,186,338.
§ 138.400 *First Offenders*	$21,665	$23,343.
§ 138.400	$22,021 up to $220,213	$23,727 up to $237,268.

Effective Date of Penalties

The revised CMP amounts for all penalties other than the penalty at 22 CFR 127.10(a)(1)(i) will go into effect on the date this rule is published. All violations for which those CMPs are assessed on or after the effective date of this rule, regardless of whether the violation occurred before the effective date, will be assessed at the adjusted penalty level. For the penalty at 22 CFR 127.10(a)(1)(i) adjusted according to section 9708 of Public Law 117-263, the new amounts will apply only to those penalties assessed for violations occurring on or after December 27, 2022.

MISSION STATEMENT:

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

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

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

Evolutions in Business

Celebrating more than 30 Years