

The Export Practitioner™

OCTOBER
2022

VOLUME 36
NUMBER 10

Timely News and Analysis of Export Regulations

INSIDE

CFIUS Reform
& Outbound
Investment
Controls

EU FDI & Supply
Chain Standards

Forced Labor –
The New FCPA

OFAC Cyber
Sanctions

BIS: Axelrod &
RAPTAC

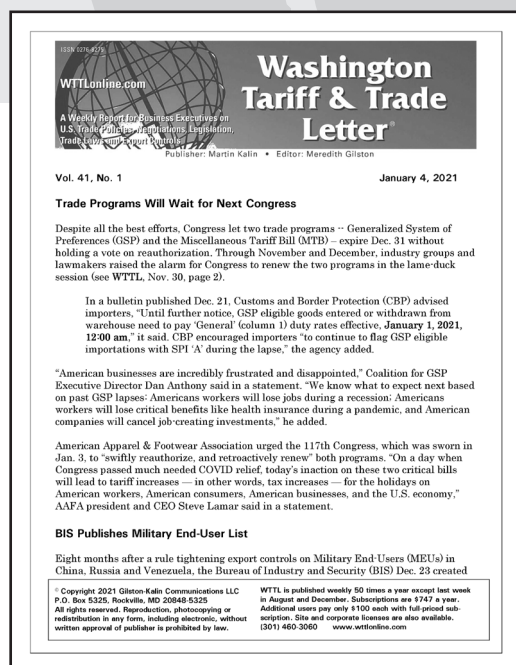
Rewards Card
Screening Fail

Los Alamos –
Beijing Axis

And More

Get the Trade News you need
EVERY WEEK with...

WASHINGTON TARIFF & TRADE LETTER



With WTTTL, you will stay ahead of developments at:

The U.S. Trade Representative's Office
Bureau of Industry & Security
International Trade Administration
International Trade Commission
Treasury's Office of Foreign Assets Control
Court of International Trade
State's Directorate of Defense Trade Controls
Export - Import Bank
Congress
Customs and Border Protection
and more...

Keep Posted on Trade Disputes and Export Opportunities in:

China | Japan | European Union | Middle East
Africa | Brazil | Central America | Mexico
Korea | Caribbean | India | Vietnam | Canada
Argentina | Colombia | Pakistan | Thailand
Morocco | Turkey | Australia

Your interest in Washington trade policy goes far beyond U.S. export controls and trade sanctions. You need to follow policy decisions, trade disputes and legislation.

You need to know what is happening on:

- Section 232 Tariffs
- Antidumping and Countervailing Duty Cases
- WTO Trade Negotiations
- Trade Sanctions on Iran, North Korea, Cuba
- Bilateral Trade Disputes
- Trade Legislation
- Customs Requirements
- Court Decisions on Trade
- Antiboycott Enforcement
- Foreign Corrupt Practices Act Cases
- Trade Promotion
- China Market Access
- NAFTA

*Every week, 50 issues a year,
Washington Tariff & Trade Letter
delivers advance, exclusive reports that provide
the full spectrum of news on trade issues of
concern to you.*

For more information on **Special Discount** and
Free Sample, Call Frank at 301-460-3060

www.WTTLOnline.com

The Export Practitioner

OCTOBER 2022

Volume 36

Number 10

Publisher

Martin Kalin

Editor

Frank Ruffing

+1.703.283.5220

fruffing@traderegs.com

The Export Practitioner

Is published monthly by

Gilston-Kalin Communications, LLC

P.O. Box 5325,

Rockville, MD 20848-5325

www.exportprac.com

On the cover:

Port of Los Angeles, California.

Credit: Art Wager, iStock

AT A GLANCE

DEPARTMENTS

4 | POLICY BRIEFS

- Biden Orders CFIUS Enhancements
- Legislative, Executive Action on Outbound Investment
- EU FDI Screening Report
- More Regulations on Supply Chains in Europe
- Labor, CBP Report on Forced Labor – The New FCPA
- National Security Review of YMTU Urged
- Crypto Regulation Gains Momentum

7 | SANCTIONS ACTIONS

- Secondary Russia Sanctions Framework Proposed
- OFAC Rewrites Cyber Sanctions Rule
- More Russia Sanctions, Guidance
- Libya, Western Balkans, Central Africa, Iran

10 | EXPORT CONTROLS

- Axelrod to Asian Forum: Be Like BIS
- RAPTAC: EU Compliance, Confidential Comments
- BIS Adds More Russians to Entity List
- BIS Calls for 1758 Controls on Bio Engineering Tools
- New BIS Rule to Aid 5G Standards Efforts
- EU Dual Use Regime Report

14 | FOCUS ON ENFORCEMENT

- Oracle Repeats the Past
- H-Bomb Site as “New Hong Kong” Yields FCPA Case
- BIS Sanctions Jailed Raytheon Engineer
- China – Federal Research Labs Axis.
- Chinese Agent in US Army Reserve

14 | PRACTITIONER PERSPECTIVE

- Doing Business Amidst Increasing Global Turbulence by Gaurav Sansanwal

White House Orders CFIUS Reform

President Biden called for government officials reviewing foreign investments to put more focus on national security risks. The September 15 executive order is the first-ever presidential directive to the inter-agency Committee on Foreign Investment in the United States.

While not expanding or limiting the legal authorities or jurisdiction of CFIUS, the order provides more direction on the national security risks that must be considered in assessing foreign investments. These include supply chain resilience, protecting sensitive data and maintaining US technological leadership, according to senior Administration officials briefing reporters.

“The administration also knows that some countries exploit our open investment ecosystem to further their own national security priorities in ways that are directly contradictory to our values and interests,” one official said. “And this new executive order is a key part of our administration’s broader effort to maintain US economic and technological leadership to protect our national security.”

The executive order expands the factors CFIUS considers to include priority emerging and critical technologies, like semiconductors, quantum technologies, biotechnology, and artificial intelligence, as well as the resilience of key supply chains, both inside and outside of the defense industrial base.

The order also identifies three additional factors for the committee to consider – aggregate industry investment trends, cybersecurity capabilities of the foreign investor and domestic entity and risks relating to American sensitive data.

White House [Fact Sheet](#) [Transcript](#) Treasury [Statement](#)

Outbound Investment Controls Endorsed

House and Senate Democratic leaders – along with a bipartisan group of lawmakers – are urging President Biden to **take executive action to keep production of critical items from moving overseas to countries like China and Russia while Congress works on legislation.**

At a Senate Banking Committee hearing September 29, “Examining Outbound Investment,” lawmakers called for legislation to be enacted before year end. The proposal by Sens. Bob Casey (D-Pa), and John Cornyn (R-Texas), would set up a reporting process for investments that may be related to national security.

“This bill would help the US better understand the risks of allowing foreign adversaries to gain access to critical capabilities and technology and to design and manufacture goods

critical to our economic and national security interests,” Sen. Casey told the committee. “Without an outbound investment screening mechanism, we cannot understand, much less safeguard, critical domestic industries and capabilities for American workers, manufacturers and innovators,” he continued. “We must avoid aiding and abetting our economic competitors and potential adversaries.”

In a letter sent to the White House before the hearing, Sens. Casey and Cornyn called for the President to move forward with executive action while deliberations continue in Congress. Executive action could then be bolstered by statutory provisions to “safeguard our national security and supply chain resiliency on outbound investments to foreign adversaries”.

Ranking Republican Pat Toomey (Pa) said he is concerned that the White House intends to rush through an executive order establishing an outbound investment regime. “An Executive Order is not a substitute for a new congressionally-passed law,” he said.

Senators call for Secondary Russian Sanctions

Senate Banking Committee members Sens. Chris Van Hollen (D-Md) and Pat Toomey (R-Pa) are proposing giving the Administration new sanctions authority to aid in efforts to sever funding to Russia’s defense sector.

At a Banking hearing last month on the effectiveness of US sanctions on Russia for its attack on Ukraine, the senators said their legislative proposal would ensure outside countries comply with a G7 initiative to cap the price of Russian oil exports. The aim of the G7 initiative is to undermine Russian profits from its oil exports. Imposing secondary sanctions on those willing to pay more than the price cap will ensure that goal is met, the senators said.

“In order to successfully enforce the price cap, it’s clear the administration requires new authority from Congress, which is exactly what our framework will provide,” the senators said in a joint statement. “By imposing strong secondary sanctions, our framework also provides the administration with the tools needed to hold accountable the financial institutions supporting those countries involved in rampant war profiteering from Russian exports.”

At the hearing, Sen. Toomey said he is particularly concerned that China and India would be willing to pay above the cap, meaning that Russia would continue to enjoy strong revenues from its oil exports.

A Treasury Department official testifying at the hearing suggested that the legislation would not be necessary. Assistant Secretary for Terrorist Financing and Financial Crimes Elizabeth Rosenberg said that price cap would provide a

strong incentive for countries outside the G7 to negotiate lower prices for the purchase of Russia oil.

The Administration has been talking about the price cap proposal and countries that purchase from Russia want to pay lower prices, she said.

EU Foreign Investment Report

The European Commission released its [Second Annual Report](#) on the screening foreign direct investments into the EU. Global foreign direct investment (FDI) inflows reached EUR 1.5 trillion in 2021, 52% more than in 2020. In 2021 over 4,000 transactions closed with foreign investors in the EU, 20.5% more than in 2020. The rebound was skewed towards the acquisition of equity stakes in existing companies, which was 32% higher compared to 2020.

The US and the UK dominated foreign transactions with 58% of the acquisitions and 60% of the greenfield investments. Information and Communications Technology (ICT) was the top sector by number of foreign acquisition (30%) and the second by foreign greenfield investments, after wholesale and retail. Manufacturing came next with 26% of all foreign acquisitions and 12% of the greenfield investments. In 2021, 53% of all foreign acquisitions in manufacturing targeted high-tech firms, compared to 45% in 2020.

Chinese greenfield investments in the EU failed to recover in 2021, and decreased by an additional 4% on a year-on-year basis, bringing Chinese greenfield investments 56% below the levels recorded in 2019

More Regulations on Supply Chains in Europe

The European Commission has unveiled a new [proposal](#) to enact a new Single Market Emergency Instrument, that empowers the bloc with “emergency powers” to regulate supply chains. The proposal will ensure that “essential goods” circulate exclusively within the European Union during what it determines to be an “emergency”. Firms would, thus, need to disclose information on production capacities and stocks of crisis-relevant goods.

The proposal is part of a larger supply resiliency trend in Europe, that is likely to increase due diligence complexities for businesses. With the measurability of supply chains having developed drastically over the last few years, addressing information gaps has become crucial.

The EC is preparing a corporate sustainability due diligence [directive](#) that would require any EU business with more than 500 employees and a global turnover of €50mn

to come up with a strategy to manage environmental and human rights standards across their supply chains, and ensure that their business model is compatible with the limiting of global warming, in line with the Paris Agreement. [\[info\]](#)

The EC also announced awards commissioning a study on effectiveness of regulations on Due Diligence Obligations for Importers of Tin, Tantalum, Tungsten and Gold (3TG) from conflict-affected and high-risk areas.

Labor, CBP Report on Forced Labor – The New FCPA

Forced Labor is a ‘Top-Tier’ compliance issue, Department of Homeland Security Undersecretary Robert Silvers told the [Wall Street Journal](#).

“Compliance professionals—and, indeed, C-suite executives—need to understand that forced labor is now a top-tier compliance issue, said Silvers. “Forced labor belongs in the same breath as FCPA. When it comes to corporate compliance programs, [the] boards of directors need to be focused on this, CEOs need to be focused on this [and], compliance teams certainly need to be laser focused on this.”

The Labor Department reports it has identified some 158 goods from 77 countries that it believes are produced by child labor or forced labor in violation of international standards. The [new report](#) adds 32 goods to the list, including two new ones – dairy products and açai berries

Labor also released its latest [report on the worst forms of child labor](#). It reviews 131 countries and territories’ child labor situations, including trafficking, debt bondage, forced labor, hazardous work, commercial sexual exploitation, and the use of children in armed conflict or illicit activities. The report details these countries’ governments efforts to eliminate child labor and provides nearly 2,200 country-specific recommendations for eliminating child labor.

In their operational statistics for August 2022, US Customs & Border Protection [reported](#) targeting 838 entries valued at more than \$266.5 million for suspected use of forced labor in the production of imported goods, including goods subject to the Uyghur Forced Labor Prevention Act and Withhold Release Orders.

Jujube Dates Spark Outrage. In a [letter](#) to CBP Commissioner Chris Magnus and OFAC Director Andrea Gacki, Rep. Jim Banks (R-Indiana) and 26 colleagues called for more aggressive enforcement of the Uyghur Forced Labor Prevention Act (UFLPA) which went into effect in June. Citing widespread availability of Xinjiang-sourced Red Jujube Dates in supermarkets and by Amazon, the lawmakers asked

for an accounting of enforcement of the UFLPA to date.

The US Department Commerce (ITA) makes available free training on the topic to help you understand the law and regulations, identify red flags, and teach you how to develop a due diligence plan. [\[Link\]](#)

China Control Drumbeat Continues

At Presstime, the White House was expected to release a new raft of restrictions on the export of advanced technologies to China. The administration's plans include blocking Chinese businesses, government research labs, and others from purchasing products that use American-made tech, The New York Times [reported](#). Expanding the use of the foreign direct product rule to block Chinese entities from buying certain chips is only one element of the strategy, the newspaper said.

Senators Call for National Security Review of YMTC

A bipartisan group of senators is urging the White House to prevent Apple from purchasing memory chips for further iPhones from Yangtze Memory Technologies Company, a state-owned company, citing national security concerns.

Senate Select Committee on Intelligence Chairman Mark Warner (D-Va) and Vice Chairman Marco Rubio (R-Fla) wrote to Director of National Intelligence Avril Haines calling for a public analysis and review of YMTC and the risks it presents to US national security. Senate Majority Leader Chuck Schumer (D-NY) and Sen. John Cornyn (R-Texas) also signed the [letter](#), released September 22.

The senators wrote that "any decision to partner with YMTC, no matter the intended market of the product offerings developed by such a partnership, would affirm and reward the PRC's distortive and unfair trade practices, which undermine US companies globally by creating significant advantages to Chinese firms at the expense of foreign competitors."

The Administration last year described YMTC as China's "national champion memory chip producer," which supports the CCP's efforts to counter U.S. innovation and leadership in this space," the senators noted.

The senators in July wrote to Commerce Secretary Gina Raimondo urging that YMTC be added to the Bureau of Industry and Security's Entity List because of the national security concerns the Chinese company poses.

Crypto Regulation Gains Momentum

Under Secretary of the Treasury Brian Nelson held a Stakeholder Meeting at the Center for a New American Security September 21st to discuss Treasury's [Action Plan to Address Illicit Financing Risks of Digital Assets](#). He noted that the use of virtual assets for illicit activities remains below the scale of traditional finance and represents a small portion of overall digital asset use, but that the increases in illicit finance in digital assets in absolute terms continues to present national security risks. **Treasury called for comments** in a September 20th Federal Register Notice [\[87 FR 57556\]](#)

Speaking at a Senate Committee on Banking, Housing and Urban Affairs hearing Sept 20th, Treasury's Assistant Secretary for Terrorist Financing and Financial Crimes said that Russia could use cryptocurrencies to evade US and other sanctions. Responding to a question from Senator Elizabeth Warren, D-Mass, Elizabeth Rosenberg acknowledged that Kremlin could turn to increased use of digital assets. In the past month, the Treasury Department has already [sanctioned](#) a virtual currency mining agency, and [designated](#) twenty-two individuals and two entities for helping Russia digitally finance the war on Ukraine.

The Financial Stability Oversight Council released its Report on Digital Asset Financial Stability Risks and Regulation. The October 3 report that large parts of the crypto-asset ecosystem are covered by the existing regulatory structure. To address regulatory gaps, the Council recommends:

- the passage of legislation providing for rulemaking authority for federal financial regulators over the spot market for crypto-assets that are not securities;
- steps to address regulatory arbitrage including coordination, legislation regarding risks posed by stablecoins, legislation relating to regulators' authorities to have visibility into, and otherwise supervise, the activities of all of the affiliates and subsidiaries of crypto-asset entities, and appropriate service provider regulation; and
- study of potential vertical integration by crypto-asset firms.

Finally, the Council recommends bolstering its members' capacities related to data and to the analysis, monitoring, supervision, and regulation of crypto-asset activities. The full report can be viewed [here](#).

In a related development, the Department of Justice has [announced](#) significant actions regarding digital assets, including the establishment of the nationwide Digital Asset Coordinator (DAC) Network to combat the threat posed by the illicit use of these assets in facilitating crime, and undermining national security. This follows the release of the first-ever

OFAC Rewrites Cyber Sanctions Rule

Treasury's Office of Foreign Assets Control (OFAC) is amending the Cyber-Related Sanctions Regulations, reissuing them in their entirety. This [final rule](#) replaces the regulations that were published in abbreviated form on December 31, 2015, and includes additional interpretive guidance and definitions, general licenses, and other regulatory provisions.

Originally issued April 1, 2015 under E.O. 13694, Treasury has authority to block property of any person determined be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located outside the United States that are likely to result in, or have contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.

Cyber-Related CAATSA Provisions – The Countering America's Adversaries Through Sanctions Act (CAATSA), established new sanctions authorities and exceptions, in addition to amending, modifying, or otherwise affecting certain Ukraine-related executive actions. Title II of CAATSA required the imposition of sanctions with respect to, among others, activities of the Russian Federation that undermine cybersecurity and persons who knowingly provide financial services in support of activities that undermine cybersecurity.

OFAC is incorporating the prohibitions in section 224(a)(1) of CAATSA, as well as the exceptions listed in section 236 of CAATSA, into the Regulations. OFAC has already implemented section 10 of SSIDES, as amended by section 228 of CAATSA, in 31 CFR part 589. OFAC anticipates incorporating the menu-based provisions of section 224(a)(2) of CAATSA into 31 CFR chapter V at a later date.

Section 578.204 of subpart B provides that all expenses incident to the maintenance of blocked tangible property shall be the responsibility of the owners and operators of such property, and that such expenses shall not be met from blocked funds, unless otherwise authorized. The section further provides that blocked **property may be sold or liquidated** and the net proceeds placed in a blocked interest-bearing account in the name of the owner of the property.

New § 578.405 explains that the prohibition on transactions with blocked persons in § 578.201 applies to **services performed by U.S. persons on behalf of a person whose property and interests in property are blocked**, as well as to services received by U.S. persons where the service is performed by, or at the direction of, a person whose property and interests in property are blocked. OFAC is redesignating the authorization for payments for legal services from funds originating outside the United States, and redesignating the authorization for emergency medical services.

OFAC is adding three new general licenses to the **Regulations**: a general license authorizing the investment and reinvestment of certain, a general license authorizing the official business of the U.S. government, and a general license authorizing certain official business of international entities and organizations. General licenses and statements of licensing policy relating to this part also may be available through the Sanctions **Related to Significant Malicious Cyber-Enabled Activities** page on OFAC's [website](http://www.treas.gov/ofac): www.treas.gov/ofac.

The rule will require most corporations, limited liability companies, and other entities created in or registered to do business in the United States to report information about their beneficial owners

FinCEN Final Rule on Beneficial Ownership Treasury's Financial Crimes Enforcement Network (FinCEN) issued a final rule establishing a beneficial ownership information reporting requirement, pursuant to the bipartisan Corporate Transparency Act (CTA). The [rule](#) will require most corporations, limited liability companies, and other entities created in or registered to do business in the United States to report information about their beneficial owners—the persons who ultimately own or control the company, to FinCEN. The requirement goes into effect January 1, 2024. [Fact Sheet](#).

OFAC Imposes More Russia Sanctions, Guidance

OFAC designated 14 persons in Russia's military-industrial complex, including two international suppliers, three key leaders of Russia's financial infrastructure, immediate family members of some of senior Russian officials, and 278 members of Russia's legislature for enabling Russia's sham referenda and attempt to annex sovereign Ukrainian territory.

In addition, OFAC issued new [guidance](#) that warns of the heightened sanctions risk that international **actors outside of Russia** would face for providing political or economic support to Russia. Frequently Asked Question (FAQ) 1091, emphasizes that OFAC is prepared to more aggressively use its existing sanctions authorities, including E.O. 13660, E.O. 14024, and E.O. 14065, to target persons — inside or outside Russia.

At a Senate Foreign Relations Committee [hearing](#) to review Russia sanctions September 28, **State's head of sanctions coordination James O'Brien** said the Administration is considering sanctions on Moscow's financial sector and high technology access. Some committee members countered that the Administration should be targeting Russia energy sector. Gaps in energy sanctions "have enabled Russia

The September 15th actions named grain thieves, collaborationist academics, kidnappers, space science centers and other advanced technology operations.

to weaponize energy supplies to Europe and generated very substantial revenues to keep Russia afloat," committee ranking Republican Jim Risch (Idaho) said.

"The administration has consistently extended the general license regarding nearly all energy-related transactions with major Russian banks giving them relief from sanctions. It is no wonder why Russian energy revenues are up and the ruble has stabilized," he continued. The G7's decision to impose an oil price cap will have no real impact, because the participating countries already have banned Russian oil imports, he said.

Treasury Assistant Secretary for Terrorist Financing and Financial Crimes Elizabeth Rosenberg argued that sanctions are having a major impact on the Russian economy. "Russia had been forced to impose draconian capital controls and is burning through its rainy-day fund, dramatically eroding its economic base and buffers in unsustainable ways. Russia will be in fiscal deficit by the end of this year," she said.

Earlier in the month, State and Treasury issued new restrictions on trade with Russian entities and persons. The September 15th actions named grain thieves, collaborationist academics, kidnappers, space science centers and other advanced technology operations. Highlights include:

- Five persons identified as supporting or enabling the theft of Ukraine's grain.
- Tetyana Tumilina, the Russian-appointed rector of Kherson State University
- Maria Lvova-Belova, Russia's Presidential Commissioner for Children's Rights who has led Russia's efforts to deport thousands of Ukrainian children to Russia.
- Ramzan Kadyrov, the leader of Russia's Republic of Chechnya, along with three wives and several daughters.

- OFAC also took action against Limited Liability Company Firdaws, which describes itself as the first "national fashion brand" of Chechnya.
- The Main Intelligence Unit (GRU), a military intelligence agency of the General Staff of the Russian Armed Forces. The GRU is being designated by the Department of State pursuant to E.O. 14024 Section 1(a)(i) for operating or having operated in the defense and related materiel sector of the Russian Federation economy. The GRU was previously designated pursuant to E.O. 13694, as amended, in 2016; pursuant to Section 224 of the Countering America's Adversaries Through Sanctions Act in 2018; and pursuant to E.O. 13382 in 2021.
- Three leading Russian military space entities that play central roles in strengthening Russia's defense capabilities.
- Advanced Technology Entities involved in semiconductors, additive manufacturing, quantum computing and physics institutes.

State [Release](#), [Factsheet](#)

OFAC Links: [Announcement: Determination Pursuant to Section 1\(a\)\(i\) of Executive Order 14024](#), a [Determination Pursuant to Section 1\(a\)\(ii\) of Executive Order 14071](#), [four related Frequently Asked Questions \(FAQs\) \(1083-1086\)](#), and [five amended FAQs \(1033, 1034, 1059, 1061, 1062\)](#)

Russia General License: Payment of Taxes, Fees, etc. GL No. 13B Issued September 8. Payments are authorized to the extent such transactions are prohibited by Directive 4 under Executive Order (E.O.) 14024, provided such transactions are ordinarily incident and necessary to the day-to-day operations in the Russian Federation.

Update and Reissue of Libya Sanctions. OFAC is amending and reissuing in their entirety the Libyan Sanctions Regulations, [31 CFR 570](#), previously published in abbreviated form in 2011. The October 3 reissuance includes additional interpretive guidance and definitions, general licenses, and other regulatory provisions to provide further guidance to the public. In E.O. 13566, the President blocked assets of Colonel Muammar Qadhafi, his government, and close associates. E.O. 13726 updated the Orders to reflect the changed situation on the ground.

The sanctions in E.O. 13566 and E.O. 13726 do not generally prohibit trade or the provision of banking or other financial services to the country of Libya. Instead, the sanctions in E.O. 13566 and E.O. 13726 apply where the transaction or service in question involves property or interests in property that are blocked pursuant to the Executive orders. OFAC is also incorporating five general licenses into the Regulations that were previously only available on OFAC's website, with modifications, including updates to the

email address for certain reporting requirements.

OFAC Western Balkans Stabilization Regulations, originally issued in 2001, have been reissued in their entirety. The measures are directed against violence in the former Yugoslav Republic of Macedonia, southern Serbia, the Federal Republic of Yugoslavia, and elsewhere in the Western Balkans region and seek to ensure the implementation of the Dayton Accords in Bosnia.

OFAC Central African Republic Sanctions of 2014 have been reissued to provide a comprehensive set of regulations that include additional interpretive guidance and definitions, general licenses, and other regulatory provisions. Issued in furtherance of the International Emergency Economic Powers Act and the United Nations Participation Act, the sanctions are intended to punitively punish the country for its failure to establish law and order and guaranteeing peace and security in the region. Unlike several other unilateral sanctions, this arms embargo has been adopted by the UN Security Council, most recently in its Resolution 2648.

Further Iran Sanctions were imposed on Iran's Morality Police and senior security officials September 23 for violence against protesters and the death of Mahsa Amini. On September 14, the LEF's Morality Police arrested 22-year-old Mahsa Amini for purportedly wearing a hijab improperly and sent her to an "educational and orientation" class at police headquarters. She was transferred to a hospital that same day in a coma and died two days later from internal injuries sustained while in Morality Police custody.

Iran Internet-based Sanctions Office of Foreign Assets Control (OFAC) issued Iran General License D-2 "General License with Respect to Certain Services, Software, and Hardware Incident to Communications" and published three Iran-related Frequently Asked Questions (1087 - 1089). The intent of the General License is to facilitate internet access as Tehran clamps down on civil unrest related to the case of Mahsa Amini.

Is a Site or Corporate License for You?

- When many individuals in your organization need to read ***The Export Practitioner*** every month, there's an easy way to make sure they get the export compliance information they must have quickly and conveniently.
- That's through a site or corporate license giving an unlimited number of your colleagues access to a print or online version of ***The Export Practitioner***.
- With a low-cost site or corporate license, you can avoid potential copyright violations and get the vital information in each issue of ***The Export Practitioner*** to everyone who should be reading it.
- **For More Information and Pricing Details, Call: 301-460-3060**

Axelrod to Asian Forum: Be Like BIS

Assistant Secretary for Export Enforcement Matt Axelrod opened the Southeast Asia Forum on Export Controls in Singapore September 15 with a recap of BIS operations and encouraged his counterparts to collaborate multi-laterally. His remarks have been edited for brevity; full Transcript [here](#).

“At the U.S. Department of Commerce we have a dedicated team of analysts and agents focused on a singularly important mission: keeping the most sensitive technologies out of the most dangerous hands. We will work tirelessly to enforce our restrictions and hold accountable those who violate them.

“My hope is that as partners in the region, we can build a collective capacity for effective enforcement to deliver this same message multilaterally. So how can we work together, both to maintain a level global playing field for industry and to ensure a safe and secure world? From my perspective, it’s through three sets of critical partnerships.

“First and foremost are partnerships with industry and academia. Industry is often our primary line of defense. After all, they’re the ones who receive the sales order. They’re the ones who evaluate whether the item, end user, and end use are appropriate.

“For our part, we have been actively working with U.S. and global industry to educate companies on compliance with our export controls and inform them of potential diversion attempts. [...] We’ve also partnered with Singapore, Malaysia, and Japan to host the JIO, which last year alone trained 1,400 exporters in the Asia-Pacific region on strategic trade controls more broadly.

“Another way we partner with industry is by helping companies that trade in U.S. items screen their end users. We also warn companies of specific diversion attempts when we receive tips through intelligence, partner, or industry channels.

“As for academia, we just launched an Academic Outreach Initiative to partner with research universities, a crucial engine of U.S. and global innovation, in order to help them better understand and comply with export controls. We are initially focusing on those universities that are involved in research and development for our Department of Defense, are researching emerging and foundational technologies, or have affiliations with parties on our Entity List.

“Our research universities are busy developing the latest and greatest technologies. But the same open and collaborative research environment that sparks such innovation can also create vulnerabilities for unauthorized technology transfer. That is why it is critical that we partner with academia to minimize risk.

“Our second critical set of partnerships involves co-

operation across our domestic law enforcement agencies. The U.S. Commerce Department, like our Singaporean colleagues, is rare among strategic trade controllers because we have both export licensing and enforcement under one roof. That co-location helps us link customs and licensing data to identify non-compliant strategic goods shipments. But even in a system such as ours, where the licensing and enforcement functions have connectivity in a single government agency, we have found that working closely with law enforcement partners across the U.S. government helps maximize the effectiveness of our enforcement efforts.

“Our domestic collaboration starts with U.S. Customs and Border Protection (CBP), which is housed in a different cabinet agency. We share strategic trade licensing information and work cooperatively with officials at CBP to identify, detain, and seize unauthorized shipments at U.S. ports and borders. Our ability to focus attention on Russia in this way simply would not be possible without our powerful partnership with our customs agency.

“We also have crucial investigative partnerships with a variety of other U.S. law enforcement agencies, like FBI, HSI, ATF, and Department of Defense investigators. It’s rare that we work a case alone. We rely on these domestic partnerships to enhance our capacity to enforce our controls. This type of partnership among domestic enforcers is a practice we believe can prove successful across the globe.

“Which brings me to the third set of partnerships – our partnerships with all of you, both bilaterally and multilaterally. We live in a world where the manufacture and distribution of advanced technologies often spans multiple countries. For all of us who work to establish and enforce strategic trade controls, that deep interconnectedness of the global supply chain means we must be deeply interconnected as well.

“A key part of that interconnection is the sharing of information and best practices. Earlier this summer, we announced the establishment of enhanced enforcement coordination efforts with both Canada and the European Commission. One foundational element of our coordination is the sharing of information to increase each other’s capability to enforce strategic controls. By combining our efforts through coordinated enforcement, we believe we expand our joint capacity to safeguard technologies from misuse and misappropriation – and help keep all of our countries safe and secure.

“There’s an old saying: “If you want to go fast, go alone. But if you want to go far, go together.” The challenges we collectively face require us to do both – to go fast and far at the same time. To me, that means we all have lots of work to do individually, within our own agencies and countries, to design, implement, and enforce effective strategic trade controls. But it also means that we have lots of work to do together, in partnership with one another.

RAPTAC: EU Compliance, Confidential Comments

The Regulations and Procedures Technical Advisory Committee held their quarterly meeting September 13 featuring a discussion with Carlo Giacomini, Director General of The European Institute for Export Compliance. The customary leadership briefing did not take place due to travel.

EIFEC is the International Standards organization for Compliance in areas that are a threat to international security and stability, such as: Nuclear, biological and chemical armaments proliferation (dual-use) implementation of the specialized compliance management framework based on International Export Compliance Standards (EIFEC EC1001 series). To process any certification or receive any assistance you must be [registered at the ECR - Export Compliance Register](#) in Brussels and approved.

Giacomini discussed the challenges of coordinating a common approach to compliance in an environment governed by multiple customs and export control regimes, with an EU overlay. To aid exporters, EIFEC has developed the [EIFEC Dual Use Index](#) which connects words with controlling codes and helps to navigate the complexity of the technical world with the controlling regulations (including where possible the National List). A group of EU national experts is reviewing the versions in German, French, Italian and Spanish.

Hillary Hess of BIS briefed participants on regulatory developments since the last meeting, reminding us that comments on proposed rulemaking can be submitted as “business confidential,” meaning firms should not withhold valuable input for fear of exposing proprietary data.

Hess also noted the impetus for the recent “Standards Rule” [\[87 FR 55241\]](#) included addressing participants in standards-setting bodies “fear of running afoul of Export Controls, and the chilling effect.”

The meeting concluded with a brief presentation by CBP on Electronic Export Manifests and the status of [enhancements](#) made.

BIS Adds More Russians to Entity List

Commerce Department’s Bureau of Industry and Security (BIS) issued a rule September 29 adding 57 entities located in Russia and the Crimea region of Ukraine to the Entity List for supporting the Russian invasion of Ukraine.

Commerce is also publishing [new guidance](#) which rules United States’ **export controls on Russia can be applied to entities in third countries** that seek to provide material

support for Russia’s and Belarus’s military and industrial sectors, including to replenish (“backfill”) technologies and other items prohibited by the United States and the 37 allies and partners that have implemented substantially similar controls.

“Russia’s attempts to illegally annex Ukrainian territory are a grotesque violation of Ukraine’s sovereignty and a blatant effort to manufacture a false reality. This phony act to legitimize the invasion cannot stand,” said **Under Secretary of Commerce for Industry and Security Alan Estevez**. “We are also further clamping down on entities that are seeking to support Russia’s military effort—inside and outside of Russia—and will continue to coordinate with our allies and partners to continue to cut Russia off further from the technologies and other items it needs to sustain its war effort.”

The entities are being added for a variety of activities contrary to U.S. national security and foreign policy interests, including acquiring or attempting to acquire U.S.-origin items in support of Russia’s military. Some are also being added for their involvement in the development of quantum computing technologies, or are otherwise important to Russia in developing advanced production and development capabilities.

Fifty of the fifty-seven entities will also be subject to the Russia/Belarus Military End User Foreign Direct Product (FDP) Rule [\[87 FR 13048\]](#) which impose severe restrictions on these entities’ access to certain foreign-produced items.

The full list of entities is included in the text of the rule released today and is available on the Federal Register’s website [here](#). An Index of resources for BIS Russia-related Export Controls can be found [here](#).

BIS Expands Export Controls on Russia & Belarus

The September 15th rule [\[87 FR 57068\]](#) imposes further export controls on industrial and commercial items that can support Russian and Belarusian military aggression against Ukraine. Specifically, the rule:

- Expands the scope of the Russian industry sector sanctions to add items potentially useful for Russia’s chemical and biological weapons production capabilities and items needed for advanced production and development capabilities that enable advanced manufacturing across a number of industries.
- Imposes controls on quantum computing-related hardware, software, and technology, which com-

plement an action taken by the Department of the Treasury to prohibit quantum computing services to Russia, as well as sanctions imposed by the Department of State on Russian companies supporting its quantum computing capabilities.

- Adds Belarus to the scope of industry sector sanctions that currently apply only to Russia.
- Expands the ‘military end user’ and ‘military-intelligence end user’ controls. Specifically, this applies the Russian/Belarusian-Military End User Foreign Direct Product (FDP) rule to entities located outside of Russia and Belarus that were previously added to the Entity List for having continued to supply Russian entities on the Entity List or are under sanctions since Russia’s further invasion of Ukraine (BIS June 28, 2022 announcement here).
- Labeling these six entities as Russian ‘military end users’ and having the Russia/Belarus-Military End User FDP rule apply to them will degrade Russia’s war efforts in Ukraine, as these entities produce items needed by the Russian and Belarusian military and industrial sectors.
- Refines existing controls on Russia and Belarus to more closely align with requirements implemented by allies by adding additional dollar value exclusion thresholds for ‘luxury goods.’
- Makes twelve additional corrections and clarifications to existing controls on Russia and Belarus.

BIS Calls for 1758 Controls on Bio Engineering Tools

Certain instruments for the automated synthesis of peptides have been identified by BIS for evaluation according to the criteria in section 1758 of the Export Control Reform Act of 2018 (ECRA) pertaining to emerging and foundational technologies. BIS is seeking public comments on the potential uses of this technology, particularly with respect to its impact on U.S. national security.

This advance notice of proposed rulemaking [87 *FR* 55930] also requests public comments on how to ensure that the scope of any controls that may be imposed on this technology would be effective (in terms of protecting U.S. national security interests) and appropriate (with respect to minimizing their potential impact on legitimate commercial or scientific applications).

The subject technology can be used to produce controlled toxins for biological weapons purposes, as well as to design novel enzymes, drugs and vaccines. *Transforma-*

tional Synthetic Biology for Military Environments initiatives by the Army Research Laboratory are applying peptide engineering to microorganisms that exhibit desirable traits, such as binding to target materials of interest, with applications in microelectronics.

Most protein toxins that are controlled under Export Control Classification Number (ECCN) 1C351 on the Commerce Control List (CCL) are over 100 amino acids in length and have an average length of 300 amino acids. Absent the imposition of additional controls on certain

New BIS Rule to Aid 5G Standards Efforts

Treasury’s The Bureau of Industry and Security (BIS) has issued an interim final rule revising the Export Administration Regulations (EAR) to authorize the release of certain technology and software in the context of standards setting and development in standards organizations.

The changes made in this interim final rule address concerns from U.S. industry and other stakeholders about whether BIS licenses are required to release low-level technology for legitimate standards activities to parties on the Entity List stemming from the listing of Huawei and a number of its non-U.S. affiliates.

“U.S. stakeholders need to be fully engaged in international standards organizations, particularly where the critical but sometimes invisible standards that they set have important national security as well as commercial implications,” said Under Secretary of Commerce for Industry and Security Alan Estevez. “Today’s rule provides much needed clarification to U.S. industry and other organizations that will allow for continued U.S. leadership in these critical bodies.”

The final rule amends the EAR to revise the standards authorization by:

- Clarifying the scope and application of standards activities covered
- Including EAR99 and Anti-Terrorism-only controlled “software” in the scope
- Authorizing the release of specified “software” and “technology” when specifically for the “development,” “production,” and “use” of cryptographic functionality; and
- Applying the scope of the authorization to all entities listed on the Entity List.

Material changes were made to Part 744 Control Policy: End-User and End-Use Based, and Part 772- Definitions of Terms. BIS is requesting comment on the revisions promulgated in this interim final rule.

More Iran Aviation Sanctions. Commerce added three Boeing 747s operated by Iranian carriers to the list of sanctioned aircraft for their involvement in providing cargo flight services on U.S.-origin aircraft to Russia. The Carriers were already subject to sanctions and the cited aircraft are legendary in MRO circles for the ruses used to keep them airborne. There are now a total of 183 aircraft identified on the list for apparent violations of U.S. export controls.

EU Dual Use Regime Report

The European Commission published a report on the implementation of Regulation (EU) 2021/821 governing the control of exports, brokering, technical assistance and transfer of dual-use items. 2021 saw the adoption of a new Export Control Regulation, which marks an important milestone in the development of EU export control policy.

Noting the role of the Trade and Technology Council (TTC) in coordinating consultations, the report addresses revisions to the EU Control List. The Regulation is binding in its entirety and directly applicable in all Member States, with provisions for the U.K. and Northern Ireland.

The Dual Use Coordination Group (DUCG) took initiatives to address certain technical implementation issues and set up dedicated expert groups to implement the requirements of the new Regulation, holding six meetings in 2021. The role of technical expert groups is now recognized in the

new Regulation, and the Surveillance Technology Expert Group (STEG) was. The STEG allows experts from Member States to contribute to the development of EU controls on exports of cybersurveillance technologies. A new Technical Expert Group on emerging technologies (ETEG) was launched as a dedicated forum for information exchange on risks associated with exports of emerging technologies and the challenges associated with their control.

The Commission, supported by the DUCG, continued to develop the Dual-Use e-System (DUeS) as the IT backbone of the EU export control network. 2021 marked the first year of operation of the dual-use eLicensing system, with its introduction in two Member States - Latvia and Romania. The eLicensing project is also developing in new directions to make controls more effective, for example, by connecting the eLicensing system with national customs systems via the Customs' Single Window environment.

In 2021, the Regulation primarily applied to the export of about 1884 dual-use items listed in Annex I (the "EU Control List") and classified in 10 categories from Annex I to Regulation (EU) 821/2021. These dual-use items relate to circa 1.000 "commodities" from the "customs nomenclature", including chemicals, metals and non-metallic mineral products, computers, electronic and optical products, electrical equipment, machinery, vehicles and transport equipment, etc. and typically fall at the high-tech end of this large, mixed commodity area.

SEE A PREVIEW OF

Mastering Deemed Exports
www.deemedexports.com

Oracle Repeats the Past

The Securities and Exchange Commission announced a settlement requiring Oracle Corporation to pay more than \$23 million to resolve charges that it violated provisions of the Foreign Corrupt Practices Act (FCPA) when subsidiaries in Turkey, the United Arab Emirates (UAE), and India created and used slush funds to bribe foreign officials in return for business between 2016 and 2019.

According to the SEC's order, Oracle subsidiaries in Turkey and UAE also used the slush funds to pay for foreign officials to attend technology conferences in violation of Oracle policies and procedures. The order found that in some instances, employees of the Turkey subsidiary used these funds for the officials' families to accompany them on international conferences or take side trips to California.

In 2012, Oracle resolved charges relating to the creation of millions of dollars of side funds by Oracle India, which created the risk that those funds could be used for illicit purposes

"The creation of off-book slush funds inherently gives rise to the risk those funds will be used improperly, which is exactly what happened here at Oracle's Turkey, UAE, and India subsidiaries," said Charles Cain, the SEC's FCPA Unit Chief. "This matter highlights the critical need for effective internal accounting controls throughout the entirety of a company's operations."

The had SEC previously sanctioned Oracle in connection with the creation of slush funds. In 2012, Oracle resolved charges relating to the creation of millions of dollars of side funds by Oracle India, which created the risk that those funds could be used for illicit purposes. In the 2012 case Oracle consented to the entry of a final judgment ordering the company to pay a \$2 million penalty and permanently enjoining it from future violations.

Rewards Card Issuer Cited for Screening Fail

As a result of deficient geolocation identification processes, Tango Card transmitted at least 27,720 stored value products to individuals with Internet Protocol (IP) and email addresses associated with Cuba, Iran, Syria, North Korea, and the Crimea region of Ukraine, in apparent violations of

multiple U.S. sanctions programs.

The Seattle company supplies and distributes rewards, often in the form of stored value cards to support client businesses' employee and customer incentive programs. While Tango Card used geolocation tools to identify transactions involving countries at high risk for suspected fraud, and had OFAC screening and Know Your Business mechanisms around its direct customers, it did not use those controls to identify whether recipients of rewards, as opposed to senders of rewards, might involve sanctioned jurisdictions.

In February 2021, one of Tango Card's clients found that several reward recipient email addresses that it had previously provided to Tango Card (and to which Tango Card had sent rewards) had top-line domains (TLDs)¹ associated with sanctioned jurisdictions. The subsequent review found that between September 2016 and September 2021, Tango Card transmitted 27,720 merchant gift cards and promotional debit cards, totaling \$386,828.65, to individuals with email or IP addresses associated with Cuba, Iran, Syria, North Korea, or the Crimea region of Ukraine.

Tango Card engaged in apparent violations of § 515.201 of the Cuban Assets Control Regulations (CACR), 31 C.F.R. part 515; § 560.204 of the Iranian Transactions and Sanctions Regulations (ITSR), 31 C.F.R. part 560; § 542.207 of the Syrian Sanctions Regulations (SSR), 31 C.F.R. part 542; § 510.206 of the North Korea Sanctions Regulations (NKSr), 31 C.F.R. part 510; and Executive Order (E.O.) 13685, "Blocking Property of Certain Persons and Prohibiting Certain Transactions with Respect to the Crimea Region of Ukraine" (the "Apparent Violations").

Following discovery of the Apparent Violations, Tango Card implemented a number of remedial measures, including geo blocking of IP and email addresses associated with sanctioned jurisdictions, hiring additional staff dedicated to improving compliance, and conducting additional sanctions compliance training. Tango Card also acquired additional screening tools and implemented new monthly lookback reports designed to identify recipients located in sanctioned jurisdictions.

While the statutory maximum civil monetary penalty applicable in this matter is \$9,168,949,062, OFAC determined that Tango Card self-disclosed the Apparent Violations and that the Apparent Violations constitute a non-egregious case. Accordingly, under OFAC's Economic Sanctions Enforcement Guidelines ("Enforcement Guidelines"), 31 C.F.R. part 501, app. A, the base civil monetary penalty applicable in this matter equals the sum of one-half of the transaction value for each apparent violation, which is \$193,414.33 reduced to \$116,048.60, reflecting the company's voluntary self-disclosure and remedial efforts put in place, including improved TLD and IP address geo-blocking; enhanced training and reporting, and hiring a consultant.

Brazilian Airline to Pay US \$41 Million in FCPA Settlement

GOL Linhas Aéreas Inteligentes S.A. (GOL), an airline headquartered in São Paulo, Brazil, will pay more than \$41 million to resolve parallel bribery investigations by criminal and civil authorities in the United States and Brazil. According to court documents, GOL entered into a three-year deferred prosecution agreement (DPA) with the Department of Justice in connection with a criminal information filed in the District of Maryland charging the company with conspiracy to violate the anti-bribery and books and records provisions of the Foreign Corrupt Practices Act (FCPA).

Between 2012 and 2013, GOL conspired to offer and pay approximately \$3.8 million in bribes to foreign officials in Brazil. Specifically, GOL caused multiple bribe payments to be made to various officials in Brazil to secure the passage of two pieces of legislation favorable to GOL. The legislation involved certain payroll tax and fuel tax reductions that financially benefitted GOL, along with other Brazilian airlines.

Pursuant to the DPA, GOL will pay a criminal penalty of \$17 million. The department has agreed to credit up to \$1.7 million of that criminal penalty against an approximately \$3.4 million fine the company has agreed to pay to authorities in Brazil in connection with related proceedings to resolve an investigation by the Controladoria-Geral da União (CGU) and the Advocacia-Geral de União (Attorney General's Office). In addition, GOL will give up approximately \$24.5 million over two years as part of the resolution of a parallel investigation by the U.S. Securities and Exchange Commission (SEC).

H-Bomb Site as “New Hong Kong” Yields FCPA Case

Two Marshall Island nationals, Cary Yan, 50, and Gina Zhou, 34, were extradited from Thailand and charged with allegedly violating the Foreign Corrupt Practices Act (FCPA), money laundering, and conspiracy to commit those offenses in connection with a scheme to bribe elected officials of the Republic of the Marshall Islands (RMI) in exchange for passing certain legislation.

Yan and Zhou allegedly offered and paid tens of thousands of dollars in bribes to elected RMI officials – including, among others, members of the RMI legislature – in exchange for supporting legislation creating a semi-autonomous region within the RMI called the Rongelap Atoll Special Administrative Region (RASAR) that would benefit the business inter-

ests of the defendants and their associates.

Promoters sought introduce tax incentives, a new tax-free shipping port and services for offshore companies registered in Rongelap. The plans sparked talk of passports for sale and an easy way to access the United States, through its Compact of Free Association agreement with the Marshall Islands, according to press reports.

Rongelap was twice evacuated after extensive nuclear tests by the United States from 1946-1958 covered its people in clouds of radioactive ash, burning them and poisoning the land for generations to come.

BIS Sanctions Jailed Raytheon Engineer

Commerce suspended the export privileges of Wei Sun for ten years. Sun is currently serving a 38-month sentence for violating the Arms Export Control Act (AECA).

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

Sun brought unclassified technical information in his company-issued computer, including data associated with an advanced missile guidance system that was controlled and regulated under the AECA and the ITAR.

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

China – Federal Research Labs Axis.

Strider Technologies has published a [report](#) documenting the talent exchange between post-doctoral fellows and researchers at the Los Alamos National Laboratory and China's military-research fusion. Since returning to China, Los Alamos alumni have helped the PRC advance key military and dual-use technologies in areas such as hypersonics, deep-earth penetrating warheads, unmanned autonomous vehicles (UAV), jet engines, and submarine noise reduction.

"Former Los Alamos scientists have made, and continue to make, considerable contributions to the PRC hypersonic, missile, and submarine programs that present an array of security risks for the United States and the entire free world. Better protection is needed for the institutions, research programs, and scientists advancing innovation in this era of strategic competition without harming open scientific collaboration," says the report.

Chinese Agent in US Army Reserve

A federal Jury convicted Ji Chaoqun for acting as an unregistered foreign agent while serving in the US Army Reserve. Ji worked at the direction of a high-level intelligence officer in the Jiangsu Province Ministry of State Security (JSSD), a provincial department of the Ministry of State Security for the People's Republic of China. A Chinese citizen residing in Chicago, Ji was tasked with providing the intelligence officer with biographical information on certain individuals for possible recruitment by the JSSD. The individuals included Chinese nationals who were working as engineers and scientists in the United States, some of whom were U.S. defense contractors.

In 2016, Ji enlisted in the U.S. Army Reserves under the Military Accessions Vital to the National Interest (MAVNI) program, which authorized the U.S. Armed Forces to recruit certain legal aliens whose skills are considered vital to the national interest. In his application to participate in the MAVNI program, Ji falsely stated that he had not had contact with a foreign government within the past seven years. In a subsequent interview with a U.S. Army officer, Ji again failed to disclose his relationship and contacts with the intelligence officer.

Ji faces up to 10 years in prison for acting within the United States as an illegal agent of the People's Republic of China and up to five years for the conspiracy and false statement offenses.

Doing Business Amidst Increasing Global Turbulence

Gaurav Sansanwal

Global Uncertainty is the New Normal

The world is in a constant state of flux. Over the last six years, companies have dealt with the adverse effects of five major “uncertainty shocks”: Brexit, the U.S. presidential election, China-U.S. trade tensions, the COVID-19 pandemic, and the Ukraine war. This global turbulence is the “new normal” and has led to increasing domestic and international policy fragmentation. Changing contours of geo-politics and geo-economics reflect that in times of global volatility, there is more to the business of business than just “business”.

In a recent report, *Harvard Business Review* has identified three overarching priorities for businesses. First, there is a need to invest in tools to track policies more closely, with special focus on the issues and regions that most affect a firm’s business. Second, flexibility can be valuable. This involves anything from signing shorter leases, leasing rather than buying property, hiring contractors rather than permanent staff, and renting rather than buying equipment. Finally, firms need to engage in contingency plans that can make them respond faster.

Supply Chain Resilience is an Immediate Priority

In its *Supply Chain Survey Report*, S&P Global Market Intelligence has identified the most challenging near-term risks to be supply chain resilience, economic fragility, and global security. Geopolitical concerns including Russia/Ukraine war and US-China trade policy came a close fourth. In this context, the immediate priority for supply chain businesses is cost optimization (raw materials, commodities, logistics), and the visibility (markets, supply, logistics) needed for better understanding of disruptions and volatility to achieve this.

Tempering Turbulence with Technology

The combined effects of prevailing uncertainty shocks have transformed the market landscape. While Brexit has introduced a more protectionist trade regime between the UK and the rest of the world, retaliatory tariffs have resulted in sharp price fluctuations. As governments pivot to new “policies of state”, the resultant “weaponization” of trade has necessitated the use of technology. The S&P survey found that data management is of importance

to over 90% of supply chain operations. Thus, timely and easy access to data and its integration across users, technologies, and the broader supply chain remains critically important.

In this background, it is helpful to consider the results of a recent industry survey by *Thomson Reuters Institute*. The survey results reveal that close to half of businesses are either behind the curve or still in the early stages of technology adoption. In what represents a peculiar challenge, almost one-fifth (19%) of businesses are still operating in highly siloed environments with disparate systems for each region and/or business unit, severely limiting their ability to share, compare, and analyze their business’s trade data.

Supplier Due Diligence & Regulatory Compliance

The challenge of regulatory compliance in this environment varies both by issue as well as region. 87% of respondents agree that supplier due diligence across the supply chain is now more important than ever due to increased regulations. According to survey results, some of the factors that are affecting global trade management business operations include new regulatory agencies, systems changes, tariffs, and sanctions. For instance, UK’s phase-out of its Customs Handling of Import and Export Freight (CHIEF) system in favor of the more technologically sophisticated Customs Declaration Service (CDS) system has been considered to be the most pressing regulatory challenge at the moment by 80% of companies in the UK and 57% in the US.

Sanctions Hurt

Similarly, sanctions — in the form of import/export limitations, tariff increases, trade status denials, port closures, financial restrictions, and other punitive actions — are now so pervasive that merely keeping up with them is a challenge for those involved in global trade compliance. Half the companies in the US, EU, and UK cited regulatory changes associated with Russia sanctions as major factors that are currently impacting their business and customs systems. In the Asia-Pacific region, however, only 26% of companies said Russia sanctions were affecting their customs systems; and in Latin America, only 20% of companies cited these sanctions as a systems concern.

US-China competition is fragmenting supply chains

Ongoing US-China trade war has affected companies has affected virtually every industry. US tariffs on steel and aluminium have prompted retaliation from countries such as Canada, Mexico, India, and Turkey. It is thus not surprising that US firms have been worst affected, with around 69% of those surveyed indicating the same. The increasing fragmentation between the two adversaries continues to accelerate the near-shoring trend. 78% of the respondents are considering supply chain diversification, with more than half noting that countries such as Vietnam and Thailand have become preferred choices. This is particularly true for larger companies that generate more than \$100 million in annual revenue.

Regulatory Complexities in Emerging Markets Subsist

Meanwhile, trade in Asia-Pacific is still fraught with complexities and nuances that businesses must navigate. More specifically, increased scrutiny around forced labor has pushed supply-chain due diligence to the top of the list of concerns companies have about conducting trade in Asia, and with China in particular. Grappling with disruptions has been equally important, with 83% of respondents stressing that disruptions are having a major impact on their businesses. Further, 65% of companies identified data residency as a significant issue in view of the restrictive data localization measures. Taking advantage of new Free Trade Agreements in the region remains a strategic business priority as well.

Further, in Latin America, regulatory compliance has become increasingly complex in response to policy changes. In Mexico, for example, the new National Customs Agency of Mexico (ANAM) has taken over many — though not all — of the tax collection, enforcement, and processing duties. Thus, transport service providers are required to include a Bill of Lading supplement with their invoices that provides detailed data on drivers, transport operators, owners, and other intermediaries. One common denominator of such regulatory changes is that countries are digitizing and integrating their customs and tax platforms to take advantage of the more centralized, sophisticated technologies that enable greater data security and transparency and are now more easily available.

Over-compliance is also a risk

In June 2022, a UN Special Rapporteur drew attention to human rights violations caused by over-compliance during checks against financial sanctions. This is a critical issue in the business sector when companies engage in excessive risk avoidance in the area of sanctions law and export controls. It is important to consider that when too much time is spent over-complying in one area, other areas come up short, leading to under-compliance that can have penal consequences. Results of a recent survey by [AEB](#) reveal particular risks with classification. Mistakes in classifying dual-use goods and screening sanctioned entities can lead to over-compliance with one regulation at the cost of the other, leading to overall under-compliance.

Difference in management approach

While 81% of the respondents in the Reuters survey agreed that the solution lay in adopting more capable global trade technologies, 74% also stressed that trade compliance and customs operations are such critical, strategic functions that they would prefer not to outsource them. This ignores the advantages of automating trade functions through a third-party service provider. If the product is properly supported, keeping track of changes in trade classifications and regulations can be made automatic. However, only 20% of companies surveyed say they rely on automated third-party intelligence to keep them up to speed on crucial compliance requirements. Almost two-thirds (65%) said they lean on the advice of consultants, 57% monitor government alerts themselves, and half obtain the information they need by conducting their own online research.

The ideal solution, thus, may be to adopt technologies that can be used in-house. An average of 57% firms are using the tools available to them through their ERP software. More than one-quarter of surveyed companies (26%) said they also use data analytics for trade analysis and supply-chain purposes. Analysts believe that there is a need to adopt a fully integrated, cloud-based data environment that gives firms complete supply-chain visibility across regions and business units. 49% of the companies surveyed have such a system, and that number jumps to 69% in the Asia-Pacific region, due to the regional influence of tech giants such as China and Japan.

Gaurav Sansanwal is an Associate Editor of the Export Practitioner. A Candidate for Master of Science in Global Business & Finance, Georgetown University, Walsh School of Foreign Service, he is licensed to practice law in India.

Subscribe Today to The Export Practitioner

Save \$100


The Export Practitioner **is the only publication devoted exclusively to reporting on U.S. export controls and trade sanctions.**

- Get fast, reliable news and analysis
- Avoid costly fines and penalties
- Move your export licenses quickly and smoothly



<https://www.exportprac.com/ht/d/Join/pid/6005>

Remember: Export Control Reforms Don't Mean Decontrol !!

 Cut out and return this money-saving coupon today.

YES, Begin my new subscription to ***The Export Practitioner*** for a full year (12 monthly issues) at the **Special Discount Price** of \$649 – a \$100 savings off the regular full price. I understand my subscription comes with a no-risk, money-back guarantee: If I ever feel it is not worth many times what I've paid, I may cancel at any time -- even the last day of my subscription -- and get a full, 100% refund!

I want to receive my issues ☐ **Online** or ☐ **Print Copy by Mail**

☐ Check Enclosed (payable to Gilston-Kalin Communications, LLC)
Charge Credit Card ☐ Visa ☐ MasterCard ☐ American Express

Card No. _____ Exp. Date _____ / _____

Name _____

Company _____

Address _____

City/State/Zip _____

Phone _____

E-Mail _____

3 Easy Ways to Subscribe

Online: www.exportprac.com
(Use coupon code: NS2022)

Phone: 703-283-5220

Mail to: Gilston-Kalin
Communications
P.O. Box 5325
Rockville, MD 20848-5325

