

The Export PractitionerTM

JULY
2022

VOLUME 36
NUMBER 7

Timely News and Analysis of Export Regulations

INSIDE

Managing
Sanctions Lists

BIS Update -
Rallying the Troops

BIS Enforcement -
Carrots & Sticks

Call to Use License
Exception STA

Anti-Boycott
Enforcement
Wakes Up

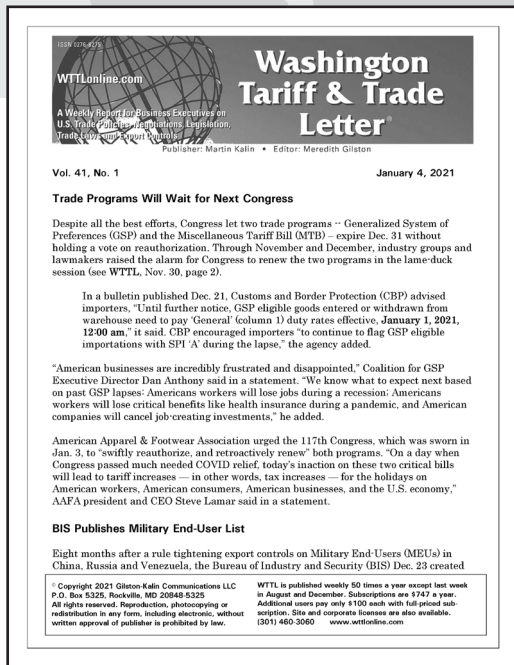
University Export
Control Focus

Monaco on
Sanctions as "New
FCPA"

Focus on
Enforcement,
and More...

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

WASHINGTON TARIFF & TRADE LETTER



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

With WTTL, 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

*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.WTTTOnline.com

The Export Practitioner

JULY 2022
Volume 36
Number 7

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

Cover:

Sorghum's cultivation has been linked by archeological research back to ancient Sudan around 6,000 to 7,000 BP. Most varieties are drought- and heat-tolerant, nitrogen-efficient, and are especially important in arid and semi-arid regions, where the grain is one of the staples for poor and rural people.
(Source: Wikipedia)

AT A GLANCE**4 | FEATURE**

Before you build a compliant screening program, you have to know the lists you're screening against. A survey of the requirement and service providers.

DEPARTMENTS**8 | POLICY BRIEFS**

- Commerce Spreads Wings, Bares Talons
- Axelrod Shines the Apple, Turns the Screws
- Anti-Boycott Enforcement to Expand
- Cap and Gown; Cloak and Dagger
- GAO Report on University Export Controls
- Senate Calls to License Export of Personal Data
- Innovation/Competes Act – Protecting Big Tech 6/13
- FMC Defines Initiatives, Compliance Role
- Ughyur Forced Labor Prevention Act
- EXIM Competitiveness Report

14 | FOCUS ON ENFORCEMENT

- More FCPA For Seamless Tube Giant Tenaris
- Aerospace Subcontractor Barred for ITAR Violations
- Warhead Contractor Pleads Guilty
- Razorback EE Prof Sentenced, Hid Patents in China
- SEC Calls Ericsson on ISIS Financing
- Thermo Fisher's Russia Distributor Charged
- Northrop Engineer Pleads Guilty to Spying for China

17 | EXPORT CONTROLS

- Kendler: Use the License Exception STA
- US Soft on Foreign Direct Product Rule?
- GAO Interagency Review of University Export Controls
- FinCEN and BIS Joint Alert

20 | TRADE SANCTIONS

- Monaco: Sanctions are "The New FCPA"
- BIS – More Russian Firms Added to Entity List
- BIS issued a final rule June 2, adding seventy-one entities located in Russia and Belarus to the Entity List
- Russia – More Airline Sanction
- Commerce added 36 entities in nine countries to the Entity List
- EU Sixth Sanctions - Chem-Bio Element
- Consolidated Guide to EU Sanctions
- OFAC - Chattel Chase Persists
- UK Adopts Stricter Rules for Sanctions Enforcement

Sanctions List Screening to Keep Pace with Evolving Sanctions Regimes

Amidst aggressive use of economic sanctions as an instrument of geostrategic competition, businesses face rising reputational, commercial, and legal risks. For actors in this polycrisis world, sanctions list screening has become a key compliance challenge. The complexity and sophistication of enforcement regimes requires firms to invest in building a coherent sanctions screening program.

Given the scale of challenge, it is not surprising that sanctions screening has been identified as a top challenge by organizations in the 2022 Thomson Reuters Anti-Money Laundering Insights Survey.¹ Similarly, 43% of those surveyed by Deloitte cited increasing complexity as the reason for rising costs of compliance, and nearly half of the executives considered themselves at high risk for exposure.²

The Importance of Using Technological Solutions

Given that compliance with varied regimes requires screening consumers, business partners, and third parties across multiple jurisdictions in the supply chain, traditional methods can no longer keep pace with the ever-changing regulatory landscape. This is because manual work leaves potential for human error in data entry, data extraction, data manipulation, screening alert review, and record keeping.

Institutionalizing processes by using specialist databases,

is therefore, critical. Technological tools such as Optical Character Recognition (OCR), Native Language Processing (NLP), Artificial Intelligence (AI), Robotic Process Automation (RPA), and machine learning are known to be helpful in transaction screening.³ Using a software can make the task of screening both internal and external data sources easier. Maintaining an automated feed of sanctions enables data management in

as much as it allows for large amounts of incoming data to be matched against screening lists. Depending on the nature of business, doing this screening in real time can be further important, especially for financial service clients.

Nearly half of executives surveyed considered themselves at high risk for exposure.

Unpacking Complexity

In order to better understand the level of complexity involved, it is important to consider that restricted parties may use sophisticated mechanisms to avoid detection—for instance, by setting up shell companies or using different naming conventions leading to incorrect spellings. Screening also requires considering the ownership and control structure of the party in question. While there are technical differences, the EU, UK and U.S. regulatory regimes largely follow the same “50 percent rule”, which requires ownership or control of more than 50 percent for the entity to be governed by the sanction.⁴

The purpose of any economic sanction is to “induce compliance with some international obligation that the tar-

¹ <https://legal.thomsonreuters.com/blog/sanctions-screening-adapting-to-a-growing-challenge/>

² <https://www2.deloitte.com/us/en/pages/advisory/articles/manage-sanctions-compliance-challenges-opportunities-survey.html>

³ <https://www.pwc.com/us/en/industries/financial-services/library/sanctions-screening-automated-solutions.html>

⁴ <https://fcpcablog.com/2022/06/13/complex-sanction-list-screenings-need-a-systematic-approach/>

get State has failed to observe”.⁵ It accordingly follows that sanctions are instruments of coercive diplomacy, employed to check the behavior of international actors. In its study of 729 publicly traceable sanction cases over the period 1950-2016, the Global Sanctions Data Base has categorized partial and complete sanctions into Trade Sanctions, Financial Sanctions, Travel Restrictions, Arms Sanctions, and Military Assistance. The objectives of these sanctions have often included more than one policy goal, and routinely relate to concerns

around democratization, human rights, ending wars, and territorial conflict. Their research has further revealed that while sanctions gradually became popular after 1950, their use has become more widespread since the early 2000s.⁶

While data collated by Statista has confirmed that Russia has now become the most-sanctioned country with more than 5,581 sanctions presently in place⁷, Global Sanctions Dashboard by Atlantic Council indicates that sanctions also continue to be imposed against countries such as the Democratic Republic of the Congo, North Korea, and Myanmar.⁸

Understanding the Global Regulatory Landscape

While sanctions imposed by the UN Security Council under Chapter VII, Article 41 apply to all nation-states, countries also impose targeted sanctions outside the scope of the UN. Given that a bulk of the unilateral, bilateral and multilateral sanctions continue to be imposed by Western nations, it is relevant to make note of the relevant regulators. While the Office of Foreign Assets Control (OFAC) does the bulk of the regulatory heavy-lifting in the US, Departments of Commerce, State, and Treasury maintain multiple export screening lists.

Russia has now become the most-sanctioned country with more than 5,581 sanctions

Similarly, EU maintains a database of sanctions imposed by the body in accordance with its Common Foreign and Security Policy, as set out in Article 21 (2) of the Treaty of EU. After Brexit, UK now maintains HM Treasury Sanctions List. In recent weeks, all bodies have indicated the need to push

for a tougher enforcement mechanism.⁹

In the US, **The Bureau of Industry and Security (BIS) at the Department of Commerce maintains the following lists:**

- Denied Persons List – Includes individuals and entities that have been denied export privileges.¹⁰
- Unverified List – Includes end-users who BIS has been unable to verify in prior transactions.¹¹
- Entity List – Includes parties whose presence in a transaction can trigger a license requirement supplemental to those elsewhere in the Export Administration Regulations (EAR).¹²
- Military End User (MEU) List – Includes parties that are prohibited from receiving items described in Supplement No. 2 of Part 744 of the EAR unless the exporter secures a license.¹³

Key sanctions lists maintained by Department of State include:

- Nonproliferation Sanctions – Includes parties that have been sanctioned under various statutes for engaging in proliferation activities.¹⁴
- AECA Debarred List – Includes entities and individuals in violation of the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR).¹⁵

5 Paul Szasz, “The Law of Economic Sanctions,” International Law Studies Series. US Naval War College 71 (1998): 455-482

6 <https://voxeu.org/article/global-sanctions-data-base>

7 <https://www.statista.com/chart/27015/number-of-currently-active-sanctions-by-target-country/>

8 <https://www.atlanticcouncil.org/blogs/econographics/global-sanctions-dashboard-russia-and-beyond/>

9 <https://www.ft.com/content/fe83c67b-5dcd-447e-aba3-34911aa5f39d>

10 <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/denied-persons-list>

11 <https://bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/unverified-list>

12 <https://bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list>

13 <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/1770>

14 <https://www.state.gov/key-topics-bureau-of-international-security-and-non-proliferation/nonproliferation-sanctions/>

15 https://www.pmdtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=c22d1833dbb8d300d0a370131f9619f0

Department of Treasury maintains the following lists:

- Specially Designated Nationals List – Includes parties who may be prohibited from export transactions based on OFAC’s regulations.¹⁶
- Foreign Sanctions Evaders List – Includes foreign individuals and entities determined to have violated, attempted to violate, conspired to violate, or caused a violation of U.S. sanctions on Syria or Iran.¹⁷
- Sectoral Sanctions Identifications (SSI) List – Includes persons operating in sectors of the Russian economy with whom U.S. persons are prohibited from transacting in.¹⁸
- Palestinian Legislative Council (PLC) List – Includes members of the PLC who were elected on the party slate of Hamas, or any other Foreign Terrorist Organization (FTO), Specially Designed Terrorist (SDT), or Specially Designated Global Terrorist (SDGT).¹⁹
- Correspondent Account or Payable-Through Account Sanctions (CAPTA) List – Includes Foreign Financial Institutions Subject to CAPTA.²⁰
- Non-SDN Menu-Based Sanctions List (NS-MBS List) – Includes persons subject to certain non-blocking menu-based sanctions that have been imposed under statutory or other authorities, including certain sanctions described in Section 235 of the Countering America’s Adversaries Through Sanctions Act (CAATSA), and the Ukraine Freedom Support Act of 2014.²¹

The advantage of using a third-party provider is the flexibility integrating with a firm’s existing ERP and CRM systems

- Non-SDN Chinese Military-Industrial Complex Companies (CMIC) – Includes persons subject to sanctions aimed at “Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies”.²²

Customs and Border Protection maintains a list of entities found to be participating in the forced labor and repression in China, the “UFLPA List.”

Exploring Screening Solutions

While the lists consolidated at government websites and in public databases such as the Global Sanctions Dashboard maintained by The Atlantic Council are up-

dated online, there is much to gain by subscribing to technological solutions that can help streamline the compliance requirements.²³

The greatest advantage of using a third-party provider of list screening is the flexibility they may afford in integrating with a firm’s existing ERP and CRM systems.

Given below is an indicative list of some firms that provide sanctions screening solutions with an eye on the regulatory and compliance requirements.

Descartes, <https://www.descartes.com/solutions/customs-and-regulatory-compliance>

Acuant, <https://www.acuant.com/sanctions-screening-pep-solution/>

CSI, <https://www.csiweb.com/how-we-help/regulatory-compliance/sanctions-screening/>

Castellum, <https://www.castellum.ai/russia-sanctions-dashboard>

Deloitte, <https://www2.deloitte.com/us/en/pages/advisory/solutions/anti-money-laundering-advisory-services.html>

Gan Integrity, <https://www.ganintegrity.com>

Lexis Nexis Risk Solutions, <https://risk.lexisnexis.co.uk>

¹⁶ <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

¹⁷ <https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists/foreign-sanctions-evaders-fse-list>

¹⁸ <https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists/sectoral-sanctions-identifications-ssi-list>

¹⁹ <https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/non-sdn-palestinian-legislative-council-ns-plc-list>

²⁰ <https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists/list-of-foreign-financial-institutions-subject-to-correspondent-account-or-payable-through-account-sanctions-capta-list>

²¹ <https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists/non-sdn-menu-based-sanctions-list-ns-mbs-list>

²² <https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/ns-cmic-list>

²³ <https://www.atlanticcouncil.org/programs/geoeconomics-center/global-sanctions-dashboard/>

Oracle, <https://www.oracle.com/industries/financial-services/aml-financial-crime-compliance/sanctions-screening/>

Protiviti, <https://www.protiviti.com/US-en/insights/sanctions-screening-systems>

Pwc, <https://www.pwc.com/us/en/industries/financial-services/financial-crimes.html>

Refinitiv, <https://www.refinitiv.com/en/risk-and-compliance/financial-crime-risk-management/sanctions-screening>

Thomson Reuters, <https://legal.thomsonreuters.com/en/products/clear-investigation-software>

Entities that are majority owned by sanctioned actors, but do not appear on a sanctions list, are subject to OFAC’s “50 Percent Rule” and its EU equivalent, and are therefore considered “sanctioned-by-law.” An example would be Ros-tec, the Russian defense conglomerate with over 800 associated entities. There are no official lists aggregating this potential exposure.

Kharon’s 50-Plus dataset provides what many in the field consider the most comprehensive coverage on entities majority owned — directly, indirectly, or in the aggregate — by sanctioned actors

<https://www.kharon.com/data/50-plus/>

Conclusion

Depending on the nature of business and the extent of attached regulatory risks, firms can consider adopting a sanctions screening program that is not only coherent, but also adaptive to the constantly evolving regulatory landscape.

Formerly the province of the multinational enterprise, given the increasing focus on enforcement, penalties involved, and the potential for business disruption, middle market and small firms are finding that adopting a coherent screening strategy has become more important than ever.



Commerce Spreads Wings, Bares Talons

The 35th Annual BIS Update Conference on Export Controls and Policy in Washington gave practitioners straight talk on industrial security after the most demanding four months in the field since the Roosevelt Administration.

Commerce Secretary Gina Raimondo opened the conference saying that “export controls are the red-hot center” of geostrategy today, and the Department is committed to its mission.

“Since the controls were put in place, global exports of semiconductors to Russia from all sources have declined by almost 90 percent, leaving Russian companies without the chips they need for a wide variety of goods, including weapons like precision guided missiles and tanks.

“Russia may be forced to ground between half and two-thirds of its commercial aircraft by 2025 in order to cannibalize them for spare parts. These controls are working. Now to sustain it.

“Yesterday [June 28], we continued to make

good on our commitment to aggressively enforce our Russia controls by identifying and adding to the Entity List various parties in China and elsewhere that contracted to supply Russia following the invasion of Ukraine.

“This is an unequivocal message to parties everywhere that the U.S. and its allies and partners will continue to closely monitor backfill attempts and will not hesitate to act swiftly to hold parties accountable who attempt to circumvent our controls.

“What if SMIC or other Chinese-based semiconductor companies are found supplying chips to Russia? We will shut them down and we can, because almost every chip in the world and in China is made using U.S. equipment and software and I intend to make good on that commitment if it's necessary.

“National security is a shared responsibility. Government plays a major role, but we need continued input, support, and diligent compliance from the private sector.”

Under Secretary of Commerce for Industry and Security Alan Estevez, with more than three decades in the Pentagon maintaining military readiness, and who boasted last month of “slowly strangling the Russian military” set the tone for the conference.

“This is the coolest job in Washington, and I’ve had cool jobs at DoD. I am the Chief Technology Protection Officer of the United States.

“In 36 years at DoD maintaining combat power, I’ve learned you never want to let your warfighters have a fair fight. Export controls are one more factor to maintain our qualitative advantage. They play a key role in protecting that advantage, to squash Russian military capability. It’s pretty hard to build 21st century weapons without semiconductors.

“With two Foreign Direct Product Rule expansions, and over 300 additions to the entity list, If I were you, I would not get on a Russian airplane.

“As to Russian steps to circumvent the controls, we are working closely with Canada Border Services and the US EU Trade & Technology Council to identify backfill entities. Those who attempt it, they’re going to be in a world of hurt.

“Winston Churchill said ‘never let a good crisis go to waste.’ Cooperation with allies, the EU, Japan,

the IPEF countries is improving from all of this. Although given Russian membership in the Wassenaar Arrangement, there is concern about updating [dual-use lists].

After an extended discussion of BIS outreach, Section 232 actions, and a plug for CHIPS act passage, Estevez told attendees: **“I can put this all very simply: 1. Russia Bad, 2. China Bad Too. 3. Allies Good. International cooperation is critical.”**

Axelrod Sweetens Carrots, Sharpens Sticks

Assistant Secretary for Export Enforcement Matt. Axelrod used his June 30 presentation at the Outlook Conference to unveil the balance of Enforcement changes he'd indicated were in the works in February, as well as new initiatives to expect.

Charging charging letters are public when filed with the Administrative Law Judge

(announced June 2). “That’s not to say we’ll always go straight to a charging letter. In appropriate cases, we will still use pre-charging letters, which are not public, and which allow us to give a company notice of what we think they’ve done wrong. In appropriate cases, pre-charging letters can be a useful tool as they allow us to have conversations and negotiations about a resolution prior to a charging letter being issued publicly.”

“Today [June 30] I am announcing four policy changes.

1. **Imposition of Significantly Higher Penalties:** To ensure that the most serious administrative violations trigger commensurately serious penalties. all appropriate cases are properly deemed “egregious,” which opens the door to more significant penalties under our regulations ensure that the existing aggravating penalty factors are applied more uniformly to escalate penalty amounts

where appropriate, which parallels how mitigating factors are currently applied to reduce penalty amounts

2. **Non-Monetary Resolution for Less Serious Violations:** To help clear through pending administrative cases where the violations do not reflect serious national security harm but do rise above the level of cases warranting a warning letter or no-action letter, we are going to offer settlement agreements that do not require monetary penalties. Instead, we will seek to resolve cases by focusing on remediation – through the imposition of a suspended denial order with certain conditions, such as training and compliance requirements. Any such resolution will be contingent on the violator’s willingness to accept responsibility, admit to the conduct, and commit to enhanced compliance measures.
3. **Elimination of “No Admit, No Deny” Settlements:** We want companies – and industry generally – to have the opportunity to learn from others and avoid making the same mistakes. When we enter a resolution, the settling party gets significant credit, in the form of a reduced penalty. But to earn that reduced penalty, there needs to be an admission that the underlying factual conduct occurred. That way, others will have a clear sense of what the company or individual did that got them into trouble and can modify their own behavior accordingly.
4. **Dual-Track Processing of Voluntary Self-Disclosures (VSDs).** For those VSDs involving minor or technical infractions, we will resolve them on a “fast-track” with a warning letter or no-action letter within 60 days of receipt of a final submission. The VSDs that are not fast-tracked will be assigned to a Special Agent and an OCC attorney. In the most serious cases, the Department of Justice’s Counterintelligence and Export Controls Section will assign an attorney as well, . By fast-tracking the minor violations while assigning specific personnel to the po-

tentially more serious ones, we will be able to use our finite resources more effectively while also allowing companies that submit more minor VSDs to receive a quicker turnaround.

“We are considering revising the EAR to recategorize the relative seriousness of the various **anti-boycott violations**. In addition, we are evaluating current penalty levels to determine whether they should be higher – both to sanction those who violate the law and to deter those who would. And, last, like I announced today with regard to export cases, we’re considering whether to eliminate “no admit, no deny” settlements in order to incentivize compliance and strengthen deterrence. I expect to have more to say about where we’ll land on these questions in the coming weeks.

Anti-Boycott Refresher - Initiatives Underway

At the BIS Rules and Procedures Technical Advisory Committee (RPTAC) meeting June 14, Kathleen Ryan of the Office of Antiboycott Compliance (OAC) briefed participants in light of the renewed interest from the Office of Export Enforcement:

If someone asks you to not deal with a certain supplier, you could not agree to that

“The anti-boycott regulations haven’t changed a lot, but we thought it would be helpful to all of you to remember there’s still out there, and given the considerations that we’re looking at, policy changes, practices in straight enforcement we thought it’d be very worthwhile to give you a little more refresher course on the anti-boycott regulations.

“We coordinate antiboycott policy with our other government agencies and partners with USTR with Treasury with State so we sort of have a whole of government and a harmonious approach to the enforcement of anti-boycott issues.

“I guess the question you all are saying is, do

these regulations have anything to do with me? Yes they do. I know the regulations have something to do for each of you because they apply to individuals, to companies, associations, even for government agencies and foreign subsidiaries.

“The first requirement is reporting if you receive a boycott request. Where would you see those boycott requests? They’re in letters of credit, in contracts in tenders. It could be in a conversation on the telephone, it could be an e-mail. If you receive a boycott request, regardless of the medium, it will be reportable to our office.

“In addition to reporting requirement, there are several prohibited actions that you cannot take. You cannot refuse to do business with the boycotted country or the blacklisted person, so if someone asks you to not deal with a certain supplier because he’s blacklisted, you could not agree to that.

“Interestingly enough, in our regulations is a prohibition against discriminatory practices. That is actually very important because it affects the employment practices of a company. If they refuse to hire a certain individual because they were blacklisted, or they were of a certain national origin, or a certain religion for a boycott reason. we can bring in administrative enforcement action against you.

“Treasury has its own set of regulations, and they maintain a list of boycotting countries as well that comports with their regulations. That list is not our list. Of course, any country on their list is a country of concern for us, but we have others that we watch that we’ve seen boycott requests coming from.

“The only thing you really need to take away from this conversation is our advice line number: 202 482 2381 It is personed all day, every day, and the duty officer does not go home until every call that day has been returned.”

Outbound Investment Screening Momentum Builds

A bipartisan group of lawmakers has finalized a revised version of the National Critical Capabilities Defense Act of 2022 (NCCDA). Building on similar provisions in the America COMPETES Act, NCCDA

seeks to establish a regulatory regime to screen outbound investments by American individuals and firms to “countries of concern”.

While the earlier provision focused on screening “transactions”, the new language is more expansive in as much as it refers to a broad range of “activities”. Drafted with the intention to protect U.S. supply chains, the new Bill has also expanded the definition of “entity of concern” to further include entities “affiliated with” or “influenced by” a country of concern. The bill, therefore, gives the proposed interagency Committee comprising of at least 12 government agencies— the wide power to prohibit or mitigate any economic activity with an entity affiliated to a country of concern.

NCCDA does, however, exempt certain types of activities from the scope of review, restricting “covered activities” to “capabilities” that include but are not limited to semiconductor manufacturing, artificial intelligence, pharmaceuticals, large-capacity batteries, and quantum technology. Recognizing the need for global cooperation, the new Act calls for “multilateral engagement” with allies and partners to counter threats posed by America’s adversaries and competitors.

Meanwhile, as lawmakers consider the nuts and bolts of the proposed legislation, the White House continues to take steps to curtail American cooperation with countries like Russia and China. As part of yet another response to the Ukrainian war, the President has announced that the government would be severely limiting its “bilateral science and technology research cooperation with the Russian government”. As momentum builds toward enacting the legal and economic architecture for the emerging great power competition, American businesses prepare to deal with more compliance requirements. (GS)

Supreme Court Limits Discovery to Courts, Arbitrators Left Out

In a decision significant for transnational dispute resolution process, the Court interpreted 28 U.S. Code (Section 1782) to hold that district courts can

order production of evidence “for use in a foreign or international tribunal” only in cases where the arbitral body is “imbued with governmental authority”.

This narrow interpretation protects businesses from exposure in international arbitrations.

It accordingly follows that American courts can only order production of evidence in cases where proceedings are underway before a formal court of law, and not in a privately held international arbitration.

This narrow interpretation of the Supreme Court in *ZF Automotive US, Inc. v. Luxshare, Ltd.*, No. 21-401 will have the effect of protecting American businesses from exposure in international arbitrations, while maintaining disclosure obligations in cross-border litigation before domestic and foreign courts of law. (GS)

Innovation/Competes Act – Protecting Big Tech

As lawmakers continue to work toward reconciling the Senate-passed United States Innovation and Competition Act (USICA) with the House-passed America COMPETES Act (H.R. 4521), a particular provision on digital governance has drawn attention. In consideration is a proposal to provide USTR the power to impose penalties on countries that have put in place illegal trade barriers in the digital sphere.

While the proposal has been designed with an eye to fight the “tide of digital censorship” in countries such as China, the broad language used therein has raised concerns. Given that many countries have enacted rules to fight disinformation, deceptive advertising, and illegal content, it is believed that the provision may hurt the right of countries to reasonably regulate digital space.

If passed in the present form, the provision against the right to regulate is likely to hit many EU policies such as the Digital Markets Act and Digital Services Act, designed to enable fair tech competi-

tion. Many lawmakers have suggested that this may have the effect of benefitting big tech companies that enjoy a near monopoly in the digital realm. (GS)

Senate Calls to License Export of Personal Data

Bipartisan legislation has been introduced in the Senate to regulate export of personal data that could potentially threaten national security. Sponsored by Senators Marco Rubio (R-Tex), Ron Wyden (D-Ore), Cynthia Lummis (R-Wyo), Sheldon Whitehouse (D-RI) and Bill Hagerty (R-Tenn), the **Protecting Americans' Data from Foreign Surveillance Act (S.4495)** seeks to block sharing of private, sensitive information with foreign adversaries.

The Act would impose penalties on senior executives “who knew or should have known..”

The draft mandates the Secretary of Commerce to restrict and regulate bulk exports of sensitive personal data to other countries by issuing licenses. While exports to “low-risk” countries would remain unrestricted, those to “high-risk” countries would be presumptively denied. If passed in the present form, the Act would impose export control penalties on senior executives “who knew or should have known that their employees were directed to illegally export personal data”.

FMC Announces Initiatives, Compliance Mandate

The Federal Maritime Commission announced three initiatives to implement the recommendations of Fact Finding 29, a two-year study of the shipping supply chain released last month.

The Commission will establish a new and permanent International Ocean Shipping Supply Chain Program, re-establish the Export Rapid Response

Team, and “Take the steps necessary for carriers, marine terminal operators, and operating seaports to employ a designated FMC Compliance Officer.”

“Compliance with Commission regulations and the statutes it administers is not voluntary or discretionary,” said an FMC official. “Ocean carriers, marine terminal operators, and operating seaports designating an FMC Compliance Officer who reports directly to the senior-most U.S.-based executive will aid in ensuring industry-wide observance of legal and regulatory requirements.”

UFLPA – Separate Entity List, PVC Gets a Pass

The Ughyur Forced Labor Prevention Act (UFLPA) became effective June 21. The Act establishes a rebuttable presumption that goods mined, produced, or manufactured wholly or in part in Xinjiang or by an entity on the UFLPA Entity List are prohibited from U.S. importation under 19 U.S.C. § 1307.

If an importer of record can demonstrate by clear and convincing evidence that the goods in question were not produced wholly or in part by forced labor, fully respond to all CBP requests for information about goods under CBP review and demonstrate that it has fully complied with the guidance provided, the Commissioner of CBP may grant an exception to the presumption.

CBP Operational Guidance for importers includes specific supply chain documentation to submit for “high-enforcement priority” commodities with a high-risk of forced labor. Examples for Cotton, Tomatoes and Polysilicon are included in the CBP Strategy Document (Xinjiang produces about one-fifth of the world’s cotton and about half of the world’s polysilicon).

The fourth “high-enforcement priority” sector-Textiles - represents a more complex enforcement challenge. A 2021 USAID-funded Sheffield Hallam University study detailed the practice of PRC textile companies that, although not using forced labor in their own mid-tier third country facilities, rely on prohibited Xinjiang raw materials or semi-finished goods.

There is no mention of Polyvinyl Chloride Resin (PVC), the manufacture of which is a major source of coerced employment and environmental damage in Xinjiang. An effective ban of UFLPA non-compliant PVC would profoundly rock the building materials supply chain.

Laura Murphy, Professor of Human Rights and Contemporary Slavery at Sheffield Hallam University recently published with others a comprehensive study of the downstream supply chain associated with Xinjiang Zhongtai Chemical Company, a Chinese government-owned petrochemical firm that is world's second largest manufacturer of PVC.

"Xinjiang Zhongtai ships to manufacturers in Vietnam, Indonesia, India, the Philippines, U.A.E., Singapore, and Russia. Those companies then ship

PVC-based flooring, pipes and fittings, and electronics coverings to the U.S., U.K., Hong Kong, Myanmar, Singapore, China, Taiwan, Belize, Nepal, Tanzania, Seychelles, Bhutan, Zambia, Sierra Leone, Indonesia, Sri Lanka, and Iraq. Caustic soda goes on to be used in manufacturing in Canada, the U.S., India, Spain, Denmark, Hong Kong, England, Russia, Germany, Mexico, Poland, Australia, and the P.R.C."

CBP will employ a "risk-based approach, dynamic in nature, that prioritizes the highest-risk goods based on current data and intelligence." According to CBP the "highest-risk goods" include those imported directly from Xinjiang into the United States and from entities on the UFLPA Entity List.

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**

More FCPA For Tenaris Tube

So much for promising not to do it again. In 2011, Argentine seamless tube maker Tenaris entered into a Non-Prosecution Agreement with the Department of Justice, and the first ever Deferred Prosecution Agreement with the SEC, because of bribery in Uzbekistan. Under the terms of that DPA, the firm paid \$5.4 million in disgorgement and prejudgment interest and agreed to pay a \$3.5 million criminal penalty in a Non-Prosecution Agreement with the Justice Department.

June 2, the SEC announced that **Tenaris will pay more than \$78 million to resolve charges that it again violated the Foreign Corrupt Practices Act (FCPA)** in connection with a bribery scheme involving its Brazilian subsidiary. Justice closed a related inquiry without taking action.

The order finds that between 2008 and 2013, approximately \$10.4 million in bribes was paid to a Brazilian government official in connection with the bidding process at Petrobras. The bribes were funded on behalf of Tenaris' Brazilian subsidiary by companies affiliated with Tenaris' controlling shareholder, Techint Group. During this period Petrobras purchased over \$1 billion in goods and services from Tenaris and affiliates.

"Tenaris failed for many years to implement sufficient internal accounting controls throughout its business operations despite known corruptions risks," said Charles Cain, Chief of the SEC Enforcement Division's FCPA Unit. "This failure created the environment in which bribes were facilitated through a constellation of companies associated with its controlling shareholder."

Tenaris consented to the SEC's order without admitting or denying the findings that it violated the anti-bribery, books and records, and internal accounting controls provisions of the Securities Exchange Act of 1934 and agreed to pay more than \$78 million in combined disgorgement, prejudgment interest, and civil penalties. The company also agreed to "comply with undertakings for a two-year period related to its ongoing remedial efforts."

Aerospace Subcontractor Barred for ITAR Violations

BIS has sanctioned a North Carolina prototyping contractor for BAE Systems, Ametek and other precision manufacturers, for illegally exporting satellite, rocket, and defense technology to China.

A Temporary Denial Order was issued June 7, giving notice to persons and companies in the United States and abroad that they should cease dealing with Quicksilver, Rapid Cut, and US Prototype in export or reexport transactions involving items, including technology or software, subject to the EAR.

Rapid Cut and affiliates received export-controlled drawings from their domestic customers to 3-D-print requested items. Despite instructions to comply with export regulations, and without their customers' advance consent or knowledge, these drawings were sent to shops in China to 3-D-print the items. The items were then imported into the United States to be provided to the ordering customers. A Rapid Cut customer reported the offenses when packaging materials identified their origin as Chinese.

Warhead Contractor Guilty

The former owner and CEO of Tungsten Heavy Powder & Parts (THPP) pleaded guilty June 9 to conspiring to commit offenses against the United States, including the unlawful exportation of defense articles on the U.S. Munitions List without first obtaining a valid license or approval from the U.S. Department of State, in violation of federal export laws pursuant to the International Traffic in Arms Regulations (ITAR).

On several occasions Joe Sery exported technical drawings from the United States via email messages to his brother in India and the People's Republic of China. An arrest warrant has been issued for the brother, Dror Sery. He is believed to be residing in Israel.

THPP is a San Diego-based company that provides tungsten fragments, sub-assemblies, and other weapon grade components for United States military contracts. Some of THPP's projects included the Hy-

personic ARRW Rapid Response Weapon, a 155-millimeter Bi-Modal Warhead, a R9E Hellfire Warhead, and an 81-millimeter mortar cowl cone.

In April 2021 THP paid a \$5.6 million fine to settle false claims act violations relating to US-funded contracts for the Government of Israel. THP falsely certified that tungsten sourced in China had been sourced, instead, in the United States. THP also falsely certified that manufacturing occurred in the United States, when in fact THP contracted with a Mexican maquiladora.

Razorback EE Prof Sentenced; Hid Patents in China

A former University of Arkansas professor of Electrical Engineering with 30 years tenure was sentenced June 16 to a year in prison plus one year of supervised release for making a false statement to the FBI about the existence of patents for his inventions in the People's Republic of China (PRC).

According to court documents, Simon Saw-Teong Ang, 64, of Fayetteville, filed 24 patents in the PRC which bear his name or Chinese birth name. The University of Arkansas, where Ang worked as a professor, required individuals such as Ang to promptly furnish to the university "full and complete" disclosures of inventions, and university policy provided that it, not individual inventors, would own all inventions created by those subject to the policy.

Despite this requirement, Ang did not disclose his Chinese patents to the university and, when interviewed by an FBI agent, lied about his involvement in the inventions. In addition, Ang also received numerous talent awards from the PRC government, which he did not list on the university's annual conflict of interest disclosure forms.

A full professor until his dismissal, Ang taught at the University since 1988. Prior to that, he spent seven years with Texas Instruments as a section chief in IC power systems development.

SEC Calls Ericsson on ISIS Financing

Ericsson announced June 9 that it had been notified that the SEC has "opened an investigation concerning the matters described in the company's 2019 Iraq investigation report, adding "too early to determine or predict the outcome of the investigation, but Ericsson is cooperating fully with the SEC."

Shareholders voted to hold CEO Börje Ekholm and the Board personally liable for the scandal.

The announcement follows the March 2 disclosure that Justice intended to find it in violation of its 2019 Deferred Prosecution Agreement (DPA) after the International Consortium of Investigative Journalists published "The Ericsson List," documenting the firm's extensive dealings with the terrorist group Islamic State in Iraq between 2011 and 2019.

In 2013 Ericsson disclosed that it was cooperating with U.S. authorities investigating bribery allegations elsewhere, resulting in a \$1 billion bribery settlement in 2019. That settlement contained no mention of Iraq. Shareholders voted March 29 to hold CEO Börje Ekholm and the Board personally liable for the scandal.

Thermo Fisher's Russia Distributor Charged

The New Hampshire-based, Russian distributor for the world's largest manufacturer of analytical instruments has been charged with regards to equipment it shipped to Russia and Ukraine from 2016 to 2019.

The charges against Intertech Corp. of Atkinson, filed June 6 by the U.S. Attorney in Concord Federal District Court, describe scientific instruments, including laser assemblies falsely identified as intended for use in aquariums, welding systems and multimedia,

and reported at artificially low values.

A search warrant unsealed in 2021 questioned 414 shipments worth \$60 million sent to Intertech's Russian affiliate, OOO Intertech Instruments, including four shipments totaling \$40 million sent to the FSB, the Russian State Security Agency. That warrant included taped phone conversations where executives allegedly discussed a plan to review records to avoid sanctions.

"After receiving the Is Informed Letter, Intertech Corporation changed its business practices to circumvent and evade the requirements set forth by the Is Informed Letter," according to the 2021 warrant.

In March 2021, BIS added OOO Intertech Instruments to the entity list, which restricts exports from companies at risk of supplying nuclear, chemical and biological weapons programs because of "proliferation activities in support of Russia's weapons of mass destruction programs."

June 24, 2002 BIS added Intertech Rus LLC and Laboratory Systems and Technologies LTD for acting as agents, fronts or shell companies for OOO Intertech Instruments.

Northrop Engineer Pleads Guilty to Spying for China

A retired U.S. Army helicopter pilot-turned-civilian-contractor pleaded guilty in federal court to acting as an unregistered agent of China and providing aviation-related information from his defense-contractor employers. He also pleaded guilty to making related false statements during national security background checks.

Shapour Moinian, 67, of San Diego, served 23 years in the Army, and then worked for defense contractors and the Department of Defense on "various projects, including a high-altitude, unmanned surveillance aircraft used by the U.S. military and various allies," according to the U.S. Attorney's Office. His roles included "F-35/F-18 System Safety Engineering at Northrop Grumman Corporation," according to Radaris.

According to his plea agreement, in 2017 while working for Northrop Grumman, Moinian was contacted by an individual in China who claimed to be working for a technical recruiting company. This person offered Moinian the opportunity to consult for the aviation industry in China. He then was issued a cell phone and other equipment to communicate with them and aid in the electronic transfer of materials and information.

In early 2018, Moinian made several internet searches regarding "sabotage vs. spying," "espionage vs. sabotage" and "selling military information to foreign country is considered as," according to the complaint filed last Fall in San Diego federal court.

Sentencing is scheduled for Aug. 29, where Moinian faces a maximum penalty of 10 years in prison and fine up to \$250,000 for acting as an agent of a foreign government, and up to five years and a \$250,000 fine for the false statements count.

Kendler: Use the License Exception STA

In a presentation to the American Association of Exporters and Importers Annual Conference June 15, Assistant Secretary for Export Administration Thea Rozman Kendler encouraged the adoption of streamlined processes offered by Commerce.

“Sometimes BIS implements solutions with good intentions that don’t land the way we expect. We created License Exception Strategic Trade Authorization (STA) eleven years ago. Our goal was to reduce licensing burdens for sensitive items to trusted destinations, facilitating compliance and protecting national security.

“Those trusted destinations are many of the same countries that joined our Russia export controls coalition. STA was – and still is -- intended to facilitate exports between the United States and our close partners by easing license burdens. The data shows you aren’t utilizing STA the way we’d hoped, and this means you’re continuing to drive the slower route.

“Some of you have followed us into the faster lanes -- Since its inception in 2011, STA has been used for approximately 145,000 shipments, for a total value of \$10.0 billion worth of transactions. Per year, that is an average of 12,000 shipments with a value of \$830 million.

“But during the same period, \$2.0 billion in exports were shipped using a BIS license even though those transactions could have been shipped using STA, which would have saved time and money for industry, not to mention BIS’s ability to more quickly process licenses for which there isn’t a substitute license exception available.

“I know there are businesses that could benefit from STA if they took the time to consider the alternate path and adapt their compliance programs. “

Cap and Gown; Cloak and Dagger

Assistant Secretary Axelrod briefed Outlook attendees on BIS’s “Academic Outreach Initiative,” addressing squarely the shortcomings highlighted in the GAO’s recent critique of enforcement agencies’ work in the university community (see below). Axelrod announced the Initiative in a speech at the National Association of College and University Attorneys Annual Conference in Pittsburgh on June 28.

“What those of us at Export Enforcement are particularly concerned about is proprietary research, which consists of research restricted from publication because it is considered confidential from a business or national security perspective, is generally controlled for either traditional export or “deemed export” purposes.

First, we will strategically prioritize engagement. We will be specifically prioritizing for engagement those universities whose work has resulted in an elevated risk profile. These are institutions that: (1) are involved in research and development for the U.S. Department of Defense; (2) have ties to foreign universities that are on the Entity List; or (3) are conducting research in sensitive technologies subject to the EAR (for example, applied laboratories conducting proprietary research on emerging technologies).

Second, we will assign “Outreach Agents” for prioritized institutions, so that each prioritized university has a dedicated point of contact. Outreach Agents will seek to meet regularly with their university counterparts, not less than once per quarter.

Third, we will offer background briefings. Our Outreach Agents will seek to brief their partner universities on known national security risks associated with specific foreign entities.

And, fourth, we will offer training. For prioritized research institutions, we will offer trainings on how export controls apply in academic settings and on applicable national security threats. In addition, our Outreach Agents will offer hands-on training to help ensure those institutions know how to vet potential partners to determine connections to parties on the Entity List or that are otherwise of concern.

GAO Interagency Review of University Export Controls

GAO released a public version of its review examining the extent to which agencies are assessing universities' risk of unauthorized deemed exports to prioritize outreach. The agencies identified outreach as a key enforcement mechanism, conceding preventing sensitive technology transfers is easier and more effective than investigating and prosecuting a violation resulting from the transfer after it has occurred.

The report finds room for improvement. For example, at the time of release, BIS Export Enforcement (EE) did not base its outreach on analysis of universities' risk levels, and had not identified any risk factors to guide its outreach priorities. The FBI and ICE applies only one risk factor. Both EE and ICE field offices said they have prioritized outreach primarily on the basis of investigative leads.

ICE and FBI have developed academia-focused outreach programs in recent years and provide academia-specific presentation templates and other materials to field offices to support outreach efforts: **ICE's Project Shield America-Academia and FBI Office of Private Sector's (OPS) Academia Program.** In addition, EE, ICE, and FBI officials present at conferences hosted by university associations, such as the Association of University Export Control Officers and the Academic Security and Counter Exploitation Program.

[At the time of release] Commerce (EE) had not undertaken broad efforts to identify risk factors that may indicate universities at greater risk for sensitive technology transfers. Moreover, field offices lack the analytical tools or personnel needed for systematic analyses that could inform outreach prioritization. Nor has EE provided specific direction to field offices on how to prioritize university outreach. [Some of these concerns were addressed in BIS June 30 Announcement - Ed.]

ICE developed a list of approximately 150 U.S. universities ranked according to one unspecified risk factor, which is not "the presence of export-controlled items or other sensitive technologies on campus." ICE officials said their selection of the single factor

they used to develop the university risk ranking was based in part on discussions with DHS's Office of Intelligence and Analysis.

GAO Identified ten risk factors that may indicate an increased risk of sensitive Technology transfers:

- Foreign students or scholars: Studies or conducts research at a graduate or postgraduate level in a sensitive field; receives research or scholarship funding from a foreign entity of concern; Is a citizen of or associated with a foreign country of concern.
- U.S. universities: Has doctoral programs with high research activity; has export-controlled items or technology on campus; receives large amounts of funding from federal agencies; uses or is developing a technology that a foreign adversary is targeting; or collaborates on research with foreign entities of concern.

Recommendations include:

- Commerce (EE) should identify relevant risk factors to identify universities at greater risk for sensitive technology transfers, including unauthorized deemed exports, shares the results of any analyses implements a mechanism to periodically assess the relevance and sufficiency of risk factors used. (These concerns have been somewhat addressed by the June 30 Announcement – Ed.)
- ICE should assess which, if any, additional risk factors are relevant for identifying universities at greater risk for sensitive technology transfers, including unauthorized deemed exports, periodically assess the relevance and sufficiency of risk factors, and share with field offices the results of any analyses aimed at identifying U.S. universities at greater risk for sensitive technology transfers.
- FBI should ensure that the appropriate offices assess which, if any, additional risk factors should be considered in identifying universities at greater risk for sensitive technology transfers, including unauthor-

ized deemed exports. And ensure that the appropriate offices periodically assess the relevance and sufficiency of risk factors considered in identifying at-risk universities.

The March report's other two objectives were to examine the challenges U.S. agencies face in their efforts to enforce export control regulations, particularly as they pertain to deemed exports at U.S. universities and examine the extent to which agencies coordinate their efforts to enforce export control regulations and share information with one another. The Departments of State, Homeland Security (DHS), Justice, and Defense deemed some of the information related to those two objectives to be sensitive information, which must be protected.

This is the second GAO report on the topic. The first report, published in May 2020, addressed the efforts that agencies undertake to educate and provide guidance to U.S. universities about export control regulations. That report also discussed the export control compliance practices of a selected group of universities. See GAO, *Export Controls: State and Commerce Should Improve Guidance and Outreach to Address University-Specific Compliance Issues*, [GAO-20-394]

White House Ends Scientific and Technological Cooperation with Russia

"Consistent with U.S. domestic and international law, we will wind down institutional, administrative, funding, and personnel relationships and research

collaborations in the fields of science and technology with Russian government-affiliated research institutions and individuals who continue to be employed by or work under the direction of those institutions."

While the announcement specifically instructs Federally Funded R&D Centers, to contact their supporting agency for guidance, "Non-government institutions should make their own determinations regarding how to proceed with contact and collaboration between the United States and Russian scientific communities, in furtherance of an open exchange of ideas within the international science and technology community."

The US is Russia's, biggest single research collaborator, according to UNESCO.

Financial Crimes Enforcement Network (FinCEN) and BIS issued a joint alert [FIN-2022-Alert003] to financial institutions, advising them to be "vigilant against efforts by individuals or entities to evade BIS export controls". The alert provides financial institutions with an overview of BIS's export restrictions to date, a list of certain commodities of concern, and other information they can use and incorporate into their risk-based screening of financial transactions. In addition, it provides select transactional and behavioral red flag indicators of export control evasion, including red flags derived from recent Bank Secrecy Act reporting.

SEE A PREVIEW OF

Mastering Deemed Exports

www.deemedexports.com



Monaco: Sanctions are “The New FCPA”

Deputy Attorney General Lisa Monaco shared her thoughts on sanctions enforcement to the GIR Live / Women in Investigations conference held June 16 in London. Highlights of her presentation include:

“One tool that is increasingly prominent at the intersection of national security challenges and corporate criminal enforcement is the department’s work on sanctions enforcement... We are pouring resources into sanctions enforcement, and you have seen and will continue to see results.

“Over the last couple of months, I’ve given notice of that sea change by describing sanctions as ‘the new FCPA.’ The growth of sanctions enforcement follows the path that the FCPA traveled before it. Both FCPA and sanctions enforcement are relevant to an expanding number of industries. They have extended beyond just U.S. actions to an increasingly multilateral enforcement regime. And they both reward companies that develop the capacity to identify misconduct within the organization, and then come forward and voluntarily disclose that misconduct to the department.

“Sanctions have been considered by some as a concern mainly for banks and financial institutions. [Now] the risk of sanctions violations cuts across industries and geographic regions... for any business with an international supply chain — sanctions should be at the forefront of its approach to compliance.

“Every company needs to be pressure-testing its sanctions compliance program, for instance through risk assessments, technology upgrades and industry benchmarking. Every board of directors of such a

company should be inquiring whether it is conducting necessary oversight of the company’s sanctions controls. Every corporate officer should be committed to ensuring they have the programs, culture, personnel, and counsel to identify problem areas and navigate the rapidly changing landscape.

“Just as the last decade saw the world of FCPA enforcement expand to foreign partners and counterparts, the months and years ahead will see the department’s sanctions teams work hand-in-glove with civil and law enforcement agencies across the world. The multilateralization of our sanctions work follows the same trajectory as our FCPA history, which grew from a largely unilateral effort by the United States to a worldwide movement to combat international corruption.

“Finally, we aim for our sanctions enforcement to incentivize companies to come forward and voluntarily disclose discovered misconduct. As with the FCPA, the department ... has a self-disclosure program to address potential criminal sanctions violations.

“For any company that thinks it may have a sanctions problem, I have a clear, unequivocal message for you: pick up the phone and call us. Do not wait for us to call you.”

EU Sixth Sanctions - Chem-Bio Element.

In addition to the widely reported restrictions on the oil trade, the most recent EU sanctions package includes a list of around 80 chemicals representing €663 million of EU exports to Russia.

The list derives from a decision of the Australia Group – the Multilateral Export Control Regime in charge of preventing the proliferation of sensitive dual-use chemicals – in response to the use of chemical weapons in Syria in 2013 and has been called the “Syria Watch List”. Further, export restrictions are extended to additional chemicals and chemical/biological equipment that might be diverted to a chemical or biological weapons program.

The export of these items to Russia would remain possible under the existing exemptions with derogations provided for non-military users and non-military uses, which cover, for example, humanitarian purposes and health emergencies as well as for medical and pharmaceutical purposes.

Consolidated Guide to EU Sanctions.

The European Commission has published a comprehensive guide to the sanctions imposed over the past four months in response to the Russian invasion of Ukraine. The 207-page document provides definitive answers to practitioners' questions, from the general (*what is the rationale behind the sanctions?*), to the specific (*is an extension of a contract considered an "ancillary contract"?*)

The document "Consolidated FAQs on the implementation of Council Regulation No 833/2014 and Council Regulation No 269/2014" has sections for Individual Measures, Finance & Banking, Trade & Customs, Energy, and Other Fields (Media, Aviation, Procurement, etc.). A copy should be on every trade lawyer's desk. https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/faqs-sanctions-russia-consolidated_en.pdf

UK Broadens Rules for Sanctions

The Office of Financial Sanctions Implementation, Government of U.K. has released new Guidance on enforcement and monetary penalties for violations relating to financial sanctions to reflect the changes introduced by the Economic Crime (Transparency and Enforcement) Act 2022. Starting June 15, **the agency will no longer have to prove that a company knew or should have known that it was in breach of sanctions.** Any breach thereof would be prosecuted on a strict liability basis, bringing the regime closer to the one in operation in the US. (GS)

Germany adopted the Sanctions Enforcement Act I (SDG I), governing the country's enforcement of EU sanctions. Asset seizures are facilitated, with amendments to money laundering and transparency protocols, as well as a "penal obligation to notify" with specific consequences for logistics providers. Among provisions, the Act allows the utilization of seized items if their safekeeping, care, or preservation would involve disproportionately high costs. Think yachts and aircraft.

OFAC - Chattel Call & Rostec Add

Under the ambitious headline "Treasury Severs More Networks Providing Support for Putin and

Russia's Elites," OFAC began the month announced the sanctioning of more persons, vessels and aircraft associated with the Putin Regime.

In addition to Maria Zakharova, the spokesperson of the Russian Ministry of Foreign Affairs; and Alexey Mordashov, the leader of Severgroup, the steel and mining concern, the announcement named the president of United Aircraft, the Russian Minister of Transport, Minister of Economic Development, Minister of Construction, Housing and Utilities, and Dmitry Grigorenko, the Deputy Prime Minister and Chief of the Government Staff of Russia.

Along with the individuals, OFAC blocked the motor yachts Graceful, Olympia, Shellest, Naga, Madame Gu, Flying Fox and Sea Rhapsody. Aircraft named include an Airbus A319-115(CJ), a Bombardier Global 6000, and an Airbus AS365 Dauphin helicopter. Most of the yachts and aircraft have deactivated their AIS transponders and have sought refuge in Russia or uncooperative havens like Turkey. **Aviation and Marine service and supply operators can expect increased scrutiny and temptation** as the roster of blocked high-value, high-maintenance vessels and aircraft swells to a measurable share of the MRO market

June 28 OFAC issued Russia-Related General License 39 (Rostec wind-down), General License 40 (Civil Aviation Safety), General License 41 (Agricultural Equipment), General License 42 Dealings with the FSB), and General License 43 (Severstal and NordGold wind-down); as well as a Determination Pursuant to Section 1(a)(i) of Executive Order 14068 (prohibiting the import of gold of Russian Federation origin), as well as related Frequently Asked Questions.

Updates to the SDN list include the addition of 70 entities, including Rostec, and 29 more individuals. **Rostec's management umbrella includes more than 800 entities across a wide range of sectors.** All entities owned 50 percent or more, directly or indirectly, by Rostec are blocked, even if not identified by OFAC

Commerce added 36 entities in nine countries to the Entity List, June 28, including five Chinese firms specifically blacklisted for allegedly supporting Russia's military and defense industrial base [87 FR 38920]. The rule includes language redesignating "The South China Sea," now named only by grid co-

ordinates. Modified were nine entities supporting the International Space Station. Former Apple camera supplier Nanchang O-Film Tech was removed from the list.

BIS issued orders denying the export privileges of three Russian airlines June 24 – Nordwind Airlines, Pobeda Airlines, and S7 Airlines – due to ongoing apparent violations of the comprehensive export controls imposed on Russia. These three Temporary Denial Orders (TDOs) terminate the right of these airlines to participate in transactions subject to the Export Administration Regulations (EAR), including exports and reexports from the United States.

Earlier, seventy-one entities in Russia and Belarus were added to the BIS Entity List June 2, Sixty-six entities were determined to be ‘military end users,’ and are receiving a “footnote 3 designation.” The footnote 3 designation means entities are subject to a license requirement for the export, reexports, exports from abroad, or transfers (in-country) of all items subject to the Export Administration Regulations (EAR), as described under the Russia/Belarus foreign “direct product” (FDP) rule. BIS will review license applications for these entities under a policy of denial. No license exceptions are available for exports, reexports, exports from abroad, or transfers (in-country) to these entities.

END NOTES

OFAC Blocked Property Reminder 31 C.F.R. § 501.603 of the Reporting, Procedures and Penalties Regulations (RPPR) requires holders of blocked property to provide the Office of Foreign Assets Control (OFAC) with a comprehensive list of all blocked property held as of June 30 of the current year by September 30.

BE-120 Benchmark Survey of Transactions in Selected Services and Intellectual Property with Foreign Persons. Commerce Bureau Economic Analysis (BEA) call for comments on changes. The BE-120 benchmark survey covers the universe of selected services and intellectual property transactions of U.S. companies with foreign persons and is BEA’s most comprehensive survey of such transactions. Comments close August 15. [87 FR 36091].

License Exemptions and Exclusions BIS to identify areas where export licensing requirements may be relaxed without jeopardizing U.S. national security or foreign policy. [87 FR 36107]

FinCEN - ANPRM for No-Action Letter Process. To solicit public comment on questions relating to the implementation of a no-action letter process at FinCEN. The addition of a no-action letter process at FinCEN could affect other forms of regulatory guidance and relief that FinCEN already offers, including administrative rulings and exceptive or exemptive relief. [87 FR 34224]

Nicaragua Treasury’s Office of Foreign Assets Control (OFAC) issued Nicaragua-related General License 3. OFAC is also publishing one related Frequently Asked Question and names have been added to the Specially Designated Nationals (SDN) list.

Iran OFAC is soliciting comments concerning their Iranian Financial Sanctions Regulations Report on Closure by U.S. Financial Institutions of Correspondent Accounts and Payable-Through Accounts [87 FR 36206].

North Korea (DPRK) White House issued Continuation of the National Emergency to deal with the unusual and extraordinary threat to the national security and foreign policy of the United States constituted by the existence and risk of the proliferation of weapons-usable fissile material on the Korean Peninsula. [87 FR 36049]

Western Balkans (Albania, Bosnia, N. Macedonia) White House issued Continuation of the National Emergency in the territory of the former Yugoslavia and the Republic of Albania (the Western Balkans) due to the undermining of post-war agreements and institutions following the breakup of Yugoslavia, as well as widespread corruption within various governments and institutions. The order was initiated June 2001. [87 FR 36051]

License Exemptions and Exclusions BIS to identify areas where export licensing requirements may be relaxed without jeopardizing U.S. national security or foreign policy. [87 FR 36107]

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

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

MASTERING EXPORT COMPLIANCE

NEWLY UPDATED!

Do your company's employees know what they should about U.S. Trade Controls?

For over a decade, our award-winning Export Compliance training videos have helped companies raise awareness and understanding of U.S. Trade Controls with easy-to-understand presentations, colorful graphics, and re-enactments. And now, we have produced our most comprehensive Mastering Export Compliance video yet, available now on DVD, BluRay, and all digital formats.

Mastering Export Compliance covers:

Overview of Export Controls
Penalties for Non-Compliance
EAR and ITAR

Red Flags for Exporters
The Role of Federal Agencies
And more!

Help your employees navigate through the U.S. Export regulatory maze with this essential tool for your company.

Contact us today at (202) 463-0904 or info@tradecompliancigroup.com.

Also available!

Mastering Import Compliance
Mastering Exports to China
Mastering Deemed Exports