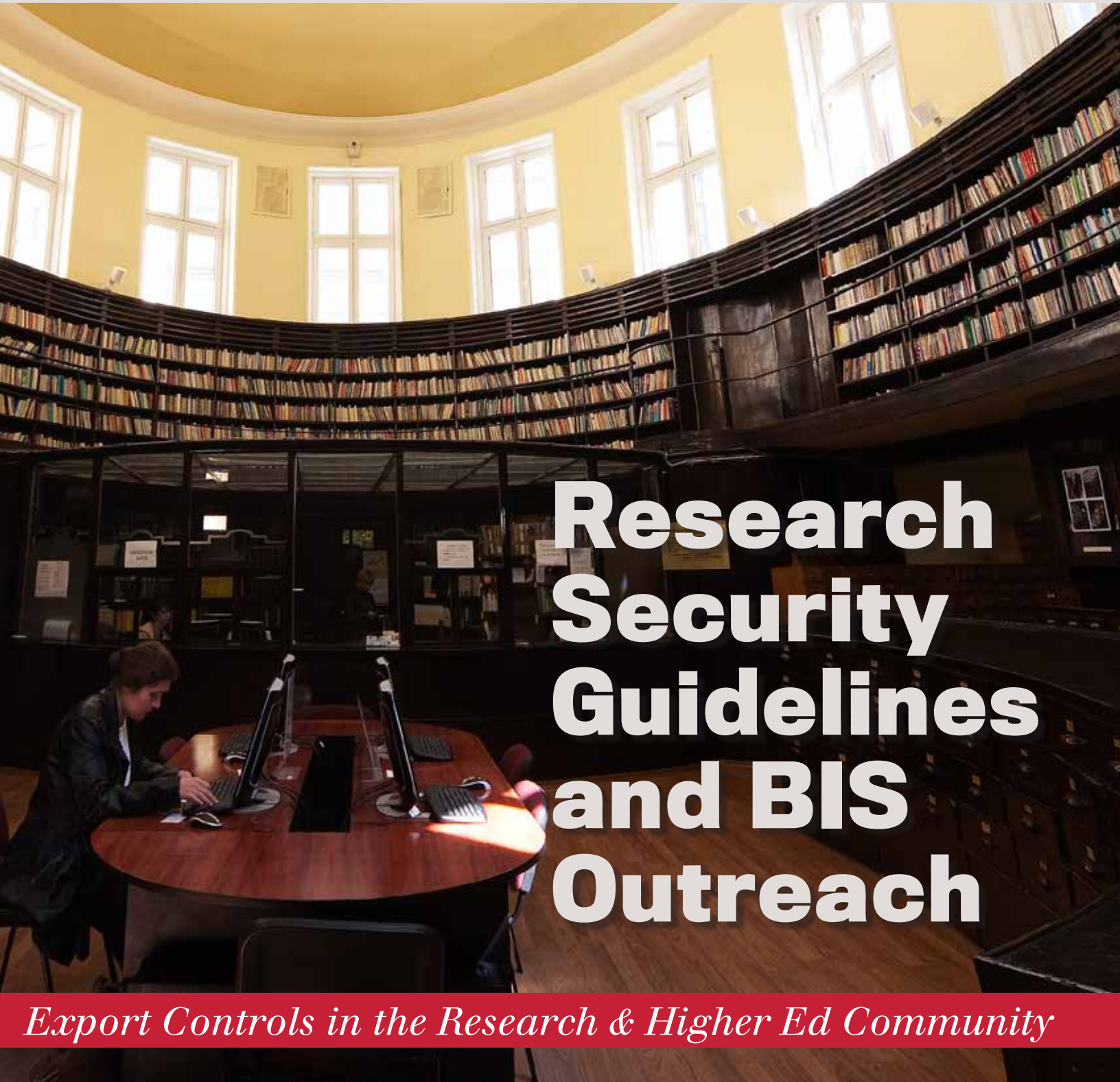
April 2023 | Vol. 37, No. 4

EP THE EXPORT PRACTITIONER™

IN THIS ISSUE:

- Justice Updates Enforcement & Compliance
- Treasury & FinCEN on Beneficial Ownership
- Trade Finance Failure Costs Wells Fargo
- Oil Price Cap a Win, Says Treasury
- Uyghur Compliance on Us All, says Expert



Research Security Guidelines and BIS Outreach

Export Controls in the Research & Higher Ed Community

WELCOME TO YOUR NEW

EXPORT PRACTITIONER™

IN PRINT | VIA EMAIL | ONLINE

VISIT ONLINE AT EXPORTPRAC.COM

FROM THE EDITOR:

After 37 years of delivering concise, timely information to the trade compliance community, The Export Practitioner has recommitted to its mission, with a new website. Enhanced graphics, richer citations, and a robust archival search, coupled with more timely updates empower readers, providing a "one-stop-shop" for export compliance professionals.

Disciplined reporting on BIS, DDTC, and OFAC ensures you are informed of the latest policy and regulatory developments, while a "Focus on Enforcement" furnishes memorable and illustrative cases to cite as you evangelize export compliance across the enterprise, from leadership to the rank and file.

We are broadening our subscriber offering, affording larger teams and entities the opportunity to share the resource, particularly in the academic and government community. Reach out to us to ensure your subscription gets to everyone who can use it.

Share your thinking with the Export Practitioner community

- We welcome original contributions from readers on all topics of interests to practitioners: Interpretation, education, and execution.
- Your submission will carry your byline. You'll get a link so you can share your story with clients and colleagues — even if they're not subscribers.

TO SUBSCRIBE, OR TO SUBMIT CONTENT:

Contact Editor Frank Ruffing at fruffing@traderegs.com, or call 301-460-3060.

EP
THE EXPORT PRACTITIONER™
APRIL 2023 | VOL. 37, NO. 4

FEATURES

Export Controls in Research & Higher Ed

- **Federal Research** Security and Academic Outreach | **4**
- **The White House releases** Research Security Programs Requirements | **4**
  while BIS expands Academic Outreach | **5**
- **Justice Turns Up Heat** on Enforcement | **8**
- **Justice officials** announced significant changes to the Corporate Enforcement Policy | **9**

POLICY

- **Yellen** on Beneficial Ownership Reform | **12**
- **FinCEN** Beneficial Ownership Guidance | **13**
- **FATF** Anti Money Laundering Guidance 9140 | **14**

ENFORCEMENT

- **Wells Fargo** Fined: Lax Sanctions Compliance | **15**
- **Dirty Miner** gets Clean Slate | **16**
- **Rio Tinto** Settles Graft Case | **17**
- **Money Transfer** Company Fined: Lax Screening | **17**
- **Montana Man** gets 20 Year Export Ban | **18**

SANCTIONS

- **Oil Price Cap** Successful says Treasury | **19**
- **Unverified List** Expands as End Use Checks Lag | **20**
- **More Iran** Aerospace Sanctions | **20**
- **Paraguay** Corruption Scandal Expands | **21**

EXPORT CONTROL

- **RAPTAC** Roundup | **2**

SUPPLY CHAIN

- **CBP** Forced Labor Expo Gets Schooled | **24**

ON THE COVER: Sofia University library. ANASTAS TARPANOV / CREATIVE COMMONS

The Export Practitioner
www.exportprac.com

Mailing Address: P.O. Box 7592, Arlington, VA 22207
Telephone: 301-460-3060
E-Mail: info@exportprac.com

Published monthly by Gilston-Kalin Communications, LLC.

Editor: Frank Ruffing,
Advisory Editor: Mary Berger
Editor Emeritus: Sam Gilston
Geneva Editor: Devarakonda Ravi Kanth
Design and Production: Creative Circle Media Solutions

Annual Subscription:
Domestic & International, $849
Site and Enterprise licenses available.
POSTMASTER: Send Address Changes to the Above Address.

ISSN 1087-478K

FEATURE

Federal Research Security Draft Released

The White House Office of Science and Technology Policy (OSTP) requests comments from the public on draft **Research Security Programs Standard Requirement** developed in response to National Security Presidential Memorandum 33 on National Security Strategy for United States Government-Supported Research and Development (R&D). Interested parties should comment on or before 5 p.m. ET June 5, 2023.

National Security Presidential Memorandum 33 directs that, "heads of funding agencies shall require that research institutions receiving Federal science and engineering support in excess of 50 million dollars per year certify to the funding agency that the institution has established and operates a research security program. Institutional research security programs should include elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training."

Stanford Main Quad. By almossawi

On January 4, 2022, the National Science and Technology Council released *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33)*, charging OSTP with "coordina[ting] activities to protect Federally funded R&D from foreign government interference, and outreach to the United States scientific and academic communities to enhance awareness of risks to research security and Federal Government actions to address these risks." A similar charge is captured in the National Defense Authorization Act of 2020.

A Draft Standard Requirement has been completed and is available for review at: https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf

As a condition for receiving and maintaining Federal science and engineering support, all covered research organizations must certify that they maintain a research security program that meets the requirements for foreign travel security, research security training, cybersecurity, and export control training,

Covered research organizations must maintain a description of the finalized research security program, made available on a publicly-accessible website, with descriptions of each item contained in this Memorandum. CUI information attached to areas such as cybersecurity or export controls need not be made public.

Foreign Travel Security International travel

policies must established or maintained for covered individuals (see Definitional Appendix) engaged in federally funded R&D who are traveling internationally for organizational business, teaching, conference attendance, research purposes, or who receive offers of sponsored travel for research or professional purposes.

Research Security Training must be implemented as a component of research security programs required for qualifying organizations in accordance with NSPM-33

Cybersecurity Implement baseline safeguarding protocols and procedures for information systems used to store, transmit, and conduct federally funded R&D. Cybersecurity standards for research security purposes will be guided by Section 10229 of the CHIPS and Science Act.

Export Control Training Organizations conducting R&D that is subject to export control restrictions must provide training to relevant personnel on requirements and processes for reviewing foreign sponsors, collaborators and partnerships, and for ensuring compliance with Federal export control requirements and restricted entities lists.

Areas subject to Federal export control requirements and restricted entities are defined through the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR). The training must emphasize that the "fundamental research" exception has explicit limitations. For example, federally funded

BIS

Axelrod Updates Academic Research Efforts

Assistant Secretary for Export Enforcement Matthew S. Axelrod reviewed his team's initiatives in the Research Community in a March 8th speech to the Academic Security and Counter Exploitation Program's Seventh Annual Seminar.

Edited for brevity.

Our research institutions are strongest and most productive when they collaborate with partners, including international ones. But at the same time, our open, collaborative research environment, which is the hallmark of American academia and one of its greatest sources of strength, also presents an inviting target for foreign adversaries who wish to exploit that environment and misappropriate our research.

In an age where you can share even the most sensitive and valuable research in an e-mail, over Zoom, or through visual inspection of certain manufacturing schematics, our research universities must be relentless in their efforts to protect themselves.

As the Assistant Secretary for Export Enforcement, I oversee a team of law enforcement agents and analysts focused on a singularly important mission: keeping our country's most sensitive technologies out of the world's most dangerous hands. One of our most important partners in this endeavor is academia.

Outreach Initiative to Expand

Last summer, we established a comprehensive effort — our "Academic Outreach Initiative" — to help academic institutions maintain their open, collaborative research environment in a way that also protects them from national security risk.

Through this initiative, we have strategically prioritized our engagement with universities whose work gives them an elevated risk profile.

When we rolled out the Initiative, we identified twenty research institutions that either possess ties to foreign universities on the Entity List; host a strategic Department of Defense University Affiliated Research Center, also known as a UARC; or conduct research in sensitive technologies subject to the Export Administration Regulations.

We're now working on identifying additional universities who meet one or more of these criteria, but who were not part of the initial group of twenty. We'll be reaching out to them in the near future about joining the Initiative. And if there's an institution that meets one of the criteria and wants to reach out to us to join, we welcome that too.

Each of the twenty institutions has been assigned a dedicated "Outreach Agent," a specific agent from their local BIS office who meets with them quarterly and

Continues on next page

Continued from previous page

serves as a resource and point of contact.

Over the past few months, we've also presented two different webinars to our partner institutions. The first focused on how export controls apply in academic settings and on ways to identify the national security threats facing universities. The second was a training on how best to conduct open-source research to better vet potential foreign partners.

This spring, we'll be offering a broader training on regulatory requirements, including fundamental research in academic settings.

Disruptive Technology Strike Force

Separate from our Academic Research Initiative, we recently launched a **Disruptive Technology Strike Force** with the Department of Justice, the FBI, and Homeland Security. The Strike Force's goal is to protect critical technological assets from being acquired by nation-state adversaries.

The types of technologies that the Strike Force will focus on are ones where our research universities are playing a critical developmental role, including advanced semiconductors, supercomputing, quantum computing, hypersonics, and biosciences related to enhancing human performance like brain control interfaces.

The Strike Force will focus enforcement resources in locations across the country to protect cutting-edge research from misappropriation.

Allied Research Security Efforts

Allied countries with world-renowned research universities face the same quandary as American ones – how to protect sensitive research from theft and diversion by nation-state adversaries while maintaining an open research environment that encourages the free exchange of ideas. And just as we at the FBI and BIS are working through that quandary with American institutions, several allied governments are doing the same in their countries.

Take the United Kingdom. There, the government published guidance on how UK export controls apply to academic research and what academics should watch out for as they conduct research with overseas partners. As noted in their Higher Education Export Control Guide and Toolkit, awareness of and guidance on export controls should form an integral part of an academic institution's research policies.

Similarly, the Australian government, in collaboration with their academic community, published the *Guidelines to Counter Foreign Interference in the Australian University Sector*, which were updated in 2021. The guidelines delineate four foundational elements for building resilience within a university: (1) governance and risk mitigation; (2) communication, training, and information sharing; (3) regular due diligence and risk assessments; and (4) cybersecurity.

The Canadian government has launched a "Safeguarding Your Research" portal, which provides information to the Canadian research community on how to safeguard their research and innovations. Canada also publishes a "Protect Your Research" guide, which is broken down by geographic region to reflect the nuances of each province and territory – highlighting specific industrial sectors, research institutions, and technology hubs in each place.

Additionally, in 2021, the Canadian government released its *National Security Guidelines for Research Partnerships*, which integrate national security considerations into the development, evaluation, and funding of research partnerships.

Fundamental research.

Scientific and technological breakthroughs are only possible because of foundational research that precedes those breakthroughs. Experimental and theoretical work must be shared, tested, and peer-reviewed. In the case of dual-use technology, the UK calls this "basic scientific research," which is undertaken solely to obtain new knowledge of the fundamental principles of phenomena or observable facts. It is not directed towards a specific practical aim or goal.

Here, the term "fundamental research" refers to scientific and technical research that is intended for publication and widespread dissemination within the academic community. As long as researchers do not accept restrictions on publication for proprietary or national security reasons, the results of fundamental research are generally not subject to the Export Administration Regulations, or EAR.

Therefore, sharing technology or software that arises during, or results from, this research will likely not require a BIS export license. The key word is "likely."

There is sometimes a misconception among professors that any research destined to be published is wholly exempt from export controls because it qualifies as fundamental research. While this is true as a general matter, there are some important exceptions that I want everyone to be aware of.

I'll touch on just two of those exceptions here – government-funded research and changes during the research cycle.

First, it is important to note that technology and software that is produced through a U.S. Government-funded research project might not be considered "fundamental research" if it is protected by government-imposed access and dissemination or other specific national security controls. These national security controls include prepublication review requirements, restrictions on publication or dissemination to non-U.S. citizens, or the restriction of participation in the project to U.S. citizens only.

And second, remember that just because your project falls within the definition of fundamental research *at the outset*, it does not mean that it will in the middle, or at the end, as publication decisions may shift.

As an example, take a project where at the beginning everyone intends that the research will be published without restrictions. The project is therefore considered fundamental research. But then, mid-project, someone sees a unique commercial use for the technology and decides that it is now proprietary information and will instead be protected.

If that happens, it would no longer be considered fundamental research, would become subject to the EAR, and may require a BIS license. For this reason, an assessment should be made at every stage or development of a research project.

In summary, even if you are conducting fundamental research, you still may be required to obtain a license if your activities fall under one of the exceptions. The question of compliance does not just end once you determine that what you're producing is considered fundamental research.

Instead, it comes down to the facts.

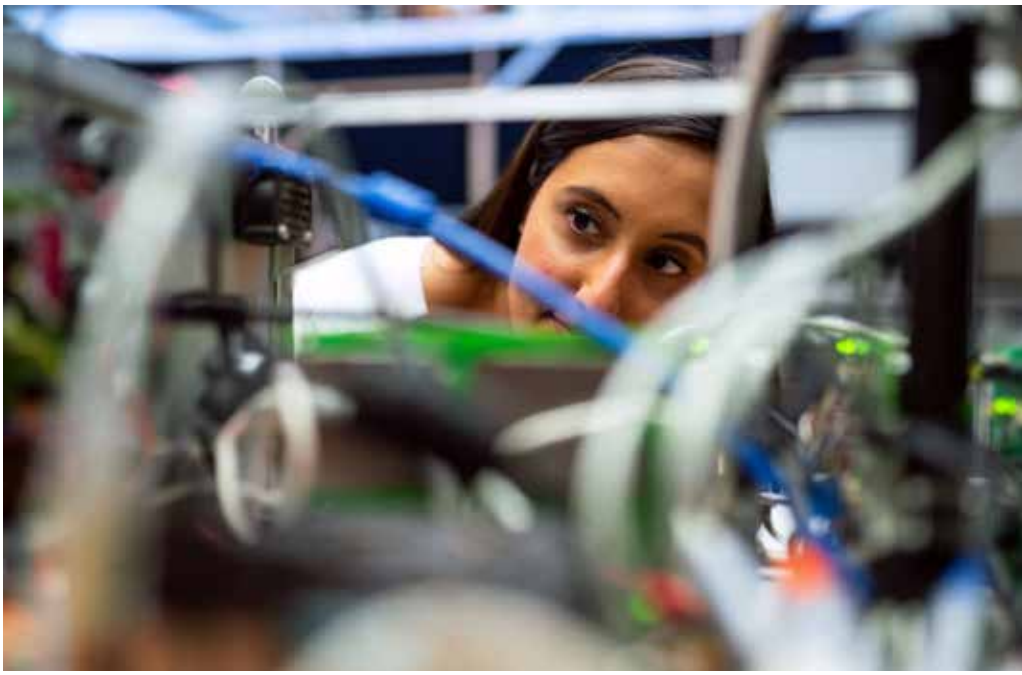
Each university research program is different. Each individual research project is different. The final determinations on fundamental research are fact specific. If you need assistance with this determination in your individual case, please reach out to your compliance team, your export control officer, and/or the BIS Office of Exporter Services. You can also choose to file an Advisory Opinion request. We have a lot of resources at your disposal so please don't hesitate to contact us.

Matt's Maxim's

If I can impart three pieces of advice to those who work in academia, it would be this:

First, export controls should be everybody's concern, not just something your compliance team thinks about. You — and I mean everyone at a

Continues on next page



"Protect your Research." From a prudential standpoint, think about the purpose of your research and the motivations of your partners.

THISISENGINEERING/ PEXELS

Continued from previous page

university, including professors, research assistants, students, counsel, academic deans, etc. — should be thinking about how export controls fit into your roles and responsibilities.

You don't need to be an expert on the EAR, but you do need to know how to spot red flags and when to reach out to your export control officer for further guidance.

Checking in with the export control officer could have prevented one Ivy League university from exporting various strains of animal pathogens without the required license to overseas research institutions in Canada, Belgium, France, and other countries. The items fell under chemical and biological weapons export controls that exist to keep the building blocks for these weapons out of the wrong hands.

University staff only realized their error during a subsequent training session on export controls. This type of unforced error — one that could have been avoided with a call to the right people at the outset — underscores how important it is that everyone think about how export controls may relate to your research and have procedures in place to guide your staff.

Second, you should always do a risk assessment before collaborating with international partners. We recommend vetting any potential partner in at least two different ways:

(1) through an open- source search, for example by using a search engine like Google, to see what is in the public domain; and

(2) checking the name of your potential partner against the Consolidated Screening List, which is a free online tool administered by the Commerce Department.

If you see any news articles, press releases, or NGO publications that link your potential partner to foreign military or defense projects, foreign intelligence or security services, or other end-users of concern, you should reach out to your compliance team, your export control officer, or BIS.

Third, as the Canadians say, "Protect your Research." From a prudential standpoint, think about the purpose of your research and the motivations of your partners. You don't want to risk your reputation by inadvertently partnering with someone who has nefarious intentions. And that's true regardless of whether you're engaged in fundamental research or not. We want you to have confidence in your collaborations and to make informed decisions concerning all of your research. If you have offers from foreign entities to purchase or invest in your research that seem too good to be true, listen to your gut and call your compliance team, your export control officer, or us at BIS.

Justice Turns up the Heat in Miami

At ABA Conference in Miami Justice announced several major initiatives related to the Corporate Enforecement Policy, in teh areas of self-disclosure, evaluation criteria for corporate compliance policies, compensation and clawbacks, and the selection of independent monitors.

In a speech on March 3, **Deputy Attorney General Lisa Monaco** delivered a message emphasizing the importance of corporate compliance and self-disclosure of misconduct. **Monaco announced that every U.S. Attorney's Office has an operative, predictable, and transparent voluntary self-disclosure program in place.** She encouraged general counsel, executives, and board members to promptly disclose criminal misconduct to the Department of Justice.

Lisa Monaco, Deputy Attorney General

Monaco also introduced a **new policy involving compensation incentives and clawbacks**, to be discussed in more detail by Assistant Attorney General Kenneth Polite. The policy includes a Pilot Program on Compensation Incentives and Clawbacks, which aims to shift the burden of corporate wrongdoing from uninvolved shareholders to those directly responsible.

Monaco announced a **surge of resources** to address the intersection of corporate crime and national security, with over 25 new prosecutors added to the National Security Division. Additionally, the Bank Integrity Unit will receive a significant investment to strengthen its capabilities in prosecuting global financial

institutions for sanctions violations.

The speech concluded with a focus on individual accountability, highlighting the department's resolve to take on challenging cases and pursue corporate crime across industries, regardless of the prominence or power of the wrongdoers.

Polite Spells Out Changes

Later in the conference, **Assistant Attorney General Kenneth Polite** emphasized the importance of international cooperation in combating crime.

He highlighted recent successful partnerships in the Diaz case and corporate resolutions such as Glencore, ABB, Danske, and Stericycle. Polite also recognized the crucial role of the financial system in global community and the need to hold companies accountable for violating U.S. financial laws. The MLARS Bank Integrity Unit has already imposed more than $13 billion in financial penalties on global financial institutions for sanctions violations since 2010, he added.

Polite also announced the reissue of the Foreign Corrupt Practices Act (FCPA) Resource Guide in Spanish and discussed **revisions to the Criminal Division's Corporate Enforcement Policy**. Polite emphasized the importance of companies voluntarily self-disclosing misconduct and fully cooperating with investigations to receive certain incentives under the policy.

He highlighted the case of Ericsson, which recently breached its 2019 deferred prosecution agreement and agreed to plead guilty to two charges filed in connection with the DPA. Polite underscored that entering a resolution is the start of a new path with a focus on cooperation and compliance.

Polite discussed significant changes to the Evaluation of Corporate Compliance Programs (ECCP), including how prosecutors will consider a corporation's approach to the use of personal devices and various communications platforms and messaging applications, including those offering ephemeral messaging.

Kenneth Polite, Assistant Attorney General

The revised ECCP will consider how policies governing these messaging applications should be tailored to the corporation's risk profile and specific business needs and ensure that business-related electronic data and communications can be preserved and accessed.

Polite also announced a pilot program to require, as part of a criminal resolution, that corporate compliance programs include compensation-related criteria and to offer fine reductions for companies that seek to clawback compensation in appropriate cases.

Finally, Polite articulated and clarified the conflict of interest obligations associated with serving as a lead monitor, or even as part of a monitor team.

He urged fellow prosecutors, defense counsel, and in-house professionals to use their mission to solve problems they see and act in a way that is meaningful, sets the right tone, and leads by example. He emphasized the need to craft and implement effective compliance programs that can detect misconduct, push to create a culture of compliance, and empower ethical employees.

Deputy Attorney General Lisa Monaco announced a surge of resources to address the intersection of corporate crime and national security, with over 25 new prosecutors added to the National Security Division.

CEP

More Polite Talk About Self-Disclosure and Declinations

Assistant Attorney General Kenneth Polite clarified the Department's new ***Corporate Enforcement Policy*** *at the Global Investigations Review DC Spring Conference, Washington, DC, March 23. Remarks Edited and condensed.*

"Many have focused on the revised policy's provisions regarding "immediate" voluntary self-disclosure and "extraordinary" cooperation and remediation. Do not lose sight of the CEP's larger context.

Since 2017, the then-FCPA CEP – which was extended to the rest of the division in 2018 – has provided that, absent aggravating factors, if a company voluntarily self-discloses misconduct, fully cooperates with our investigation, and timely and appropriately remediates, it can earn a presumption of a declination.

The new CEP released in January does not disturb this well-trodden path to a declination. Instead, our revisions provide an additional avenue toward a declination for companies that voluntarily self-disclose, cooperate, and remediate but have aggravating factors and would otherwise be ineligible for a presumption of declination.

It is only in that context – where a company has aggravating factors yet seeks a declination – that it must demonstrate "immediate" voluntary self-disclosure, "extraordinary" cooperation and remediation, and a fully functioning compliance program at the time of the misconduct and the disclosure.

To be sure, the revised CEP specifies a new path for a declination where there are aggravating factors. As I mentioned, this may occur where the company immediately self-discloses misconduct, provides extraordinary cooperation and remediation, and has an effective compliance program in place at the time of the misconduct and the time of the disclosure.

But we understand that companies may wish for more to guide their decision-making now. A company with aggravating factors that is contemplating self-disclosure may want to know what exactly it needs to do to receive a declination under the revised CEP.

To receive credit for extraordinary cooperation, companies must go above and beyond the criteria for full cooperation set out in our policies — not just run of the mill, or even gold-standard cooperation, but truly extraordinary. And I noted some concepts — immediacy, consistency, degree, and impact — that will help to inform our approach to assessing what is "extraordinary."

As with cooperation, "extraordinary" remediation must go beyond the policy's criteria. There are often many fact-specific ways companies can remediate. The most effective remediation, however, includes conducting root cause analyses and taking action to prevent the misconduct from occurring, even in the face of substantial cost or pressure from the business.

Therefore, regardless of the specific acts taken, when assessing whether remediation has been "extraordinary," we will consider if the action has been comprehensive, tailored to the causes of the misconduct under investigation as well as other potential wrongdoing, and able to prevent it from recurring. For that is our ultimate aim: to incentivize companies to invest heavily in designing and implementing effective compliance programs that can deter, prevent, and, if necessary, detect criminal conduct.

Indeed, remediation can take such different forms that, when evaluating corporate compliance programs, there is no one-size-fits-all approach. We have consistently decided not to offer prescriptive guidance but instead, through our Evaluation of Corporate Compliance Programs (ECCP), established criteria and questions that our prosecutors can ask when assessing these programs.

Of course, our recently announced Pilot Program is new. Over the next three years, we will require companies that enter into criminal resolutions to implement compliance-related criteria in their compensation systems and will offer fine reductions to companies that seek in good faith to clawback compensation from appropriate individuals.

Through all of this work, one thing is clear. The Criminal Division has been the preeminent leader not only in corporate enforcement, but also in crafting white-collar policy for prosecutors. For years, our prosecutors have considered how we can best achieve our mission and put those ideas into practice. We have used these experiences to determine how we can encourage good corporate citizenship, incentivize the investment in robust compliance programs, and further our primary goal of individual accountability.

JUSTICE

Updated Guidelines for Evaluating Corporate Compliance Programs

The U.S. Department of Justice Criminal Division has updated its guidelines for evaluating corporate compliance programs, which prosecutors use to determine whether to bring charges against a company and negotiate plea or other agreements. The guidelines include factors such as the adequacy and effectiveness of a corporation's compliance program at the time of the offense and its remedial efforts to improve the program.

The guidelines, which were updated in March 2023, are intended to help prosecutors make informed decisions about the appropriate form of resolution or prosecution, monetary penalties, and compliance obligations for a corporation.

The Criminal Division recognizes that each company's risk profile warrants particularized evaluation, but has identified **three fundamental questions that prosecutors should consider:**

- **Is the corporation's** compliance program well designed?
- **Is the program** being applied earnestly and in good faith, with sufficient resources and empowerment to function effectively?
- **Does the corporation's** compliance program work in practice?

To answer these questions, prosecutors may evaluate the company's performance on various topics, including risk management, policies and procedures, training and communication, reporting structure and investigation process, due diligence for third-party relationships and mergers and acquisitions, and consequences for non-compliance.

While the sample topics and questions provided by the Criminal Division are not a checklist or formula, they offer guidance for evaluating a company's compliance program on a case-by-case basis. The Criminal Division acknowledges that some topics may be more salient than others given the particular facts of a case.

Summary of Guidelines

➤ **To enhance your corporate compliance program**, consider the following advice for leadership:

- **Ensure the program** is comprehensive and well-integrated, with clear messages against misconduct and policies that address identified risks.
- **Regularly review and update** the compliance program, tailoring it to the company's risk profile and business needs.
- **Implement risk management** processes, risk-tailored resource allocation, updates and revisions, and incorporate lessons learned from your own and others' experiences.
- **Design comprehensive** and accessible policies and procedures, and ensure they are integrated into the company's operations.
- **Provide tailored training** and communication, establish a confidential reporting structure, and maintain an effective investigation process.
- **Implement risk-based due diligence** for third-party relationships and comprehensive due diligence for mergers and acquisitions.
- **Allocate sufficient resources** and empower the compliance function to operate effectively, ensuring commitment from senior and middle management.
- **Evaluate the compliance** function's structure, seniority, experience, qualifications, funding, data resources, access, and autonomy.
- **Establish clear incentives** for compliance and disincentives for non-compliance, including consistent disciplinary measures and financial incentive systems.
- **Continuously improve and sustain** the compliance program through periodic testing and review, internal audits, and control testing, fostering a culture of compliance.

'By one estimate, illicit actors laundered at least $2.3 billion through U.S. real estate between 2015 and 2020.'

JANET YELLEN, TREASURY SECRETARY

Yellen on Beneficial Ownership Reform

Multilateral commitment announced

Treasury Secretary Janet Yellen announced a commitment by the United States and more than twenty foreign governments to enhance beneficial ownership transparency. [edited for brevity]

At the first Summit for Democracy in 2021, I described corruption as a "common adversary" for democracies everywhere. Since then, we have all witnessed the dangers and damage that this adversary has inflicted across the globe.

Corruption has fueled the rise of kleptocratic regimes that are divorced from the interests of their own citizens. Corruption allowed Vladimir Putin and Russian oligarchs to squander their nation's wealth to fund their illegal war against Ukrainian civilians. Last month, Corruption has also fueled political dysfunction in countries like Lebanon. It has subjected nations to cycles of deteriorating economic conditions.

We know that corruption's effects spill across borders. We have seen corrupt foreign officials bury stolen funds in U.S.-based shell companies; kleptocrats launder kickbacks through anonymous purchases of foreign real estate; and elites move corrupt proceeds through complicit or unwitting financial gatekeepers like attorneys or wealth managers.

I'd like to focus today on what we are doing both at home and with partners across the world to tackle corruption.

Domestic Efforts

Over the last few years, the Treasury Department has been hard at work building key infrastructure to fortify our financial system — and those investments will soon begin to pay off.

By this time next year, it will be more difficult for corrupt and criminal actors to hide their identities and wealth behind anonymous shell companies in the United States. Starting January 1, 2024, many companies formed or operating in the United States will be required to report information about their beneficial owners — that is, the real people who own or control a company.

Unmasking shell corporations is the single most significant thing we can do to make our financial system inhospitable to corrupt actors.

Treasury has a lot of work to do to realize this promise – including by advancing additional rulemakings that need to be calibrated carefully. The database must be highly useful to all of its stakeholders. It must also ensure that firms—some of them very small businesses—understand their obligations.

We're putting a particular focus on excluding corrupt actors from investing in, profiting from, and laundering money through investment firms as well as through purchases of U.S. real estate.

By one estimate, illicit actors laundered at least $2.3 billion through U.S. real estate between 2015 and 2020. And the real number is almost

certainly much higher. Treasury is working to remove that anonymity — and capture information about residential and commercial transactions not covered by our Bank Secrecy Act or beneficial ownership regimes.

International Efforts

Without a strong and unified global approach, corrupt actors will continue to exploit financial loopholes and lightly regulated jurisdictions. We're particularly focused on raising international standards for anti-money laundering at forums like the Financial Action Task Force, or FATF.

➤ **In October, the FATF agreed** to undertake three major projects to enhance global anti-corruption efforts.

• **First,** it will enhance assessments of countries' implementation of the **United Nations Convention** Against Corruption.

• **Second**, it is addressing the use of "**golden passports**" by corrupt actors to hide their activities through the use of new identity documents.

• **And third**, it is working to reduce the ability of corrupt actors to take advantage of **financial gatekeeping professions** across all jurisdictions.

I am also pleased to launch today a commitment by the United States and more than twenty foreign governments and authorities participating in this summit to enhance beneficial ownership transparency.

I want to specifically highlight the Financial Transparency and Integrity Cohort, which was launched at the first Summit. This cohort has brought together a broad range of stakeholders to consult and coordinate on anti-corruption issues.

I'm confident that we can work to build a level playing field. This is our responsibility as democracies: to forge a world in which free institutions can thrive and in which those who play by the rules have the best chances of success.

Full text: https://home.treasury.gov/news/press-releases/jy1371

FINCEN

Beneficial Ownership Guidance

Reporting rules change January 1, 2024

Financial Crimes Enforcement Network (FinCEN) published its first set of guidance materials to aid the public, and in particular the small business community, in understanding upcoming beneficial ownership information (BOI) reporting requirements taking effect on January 1, 2024.

The new regulations require many 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.

A proposed reporting form that would give companies the option to say that they were unable to identify their owners, and to mark "unknown" with respect to key information about any owners has drawn criticism, according to the *Wall Street Journal*.

"FinCEN is working to issue an updated beneficial ownership information reporting form as soon as possible," Himamauli "Him" Das, the acting director of the Treasury's Financial Crimes Enforcement Network, said in a statement.

The following materials are now available on FinCEN's beneficial ownership information reporting webpage, www.fincen.gov/boi:

Answers to Frequently Asked Questions about the reporting requirement.

One Pagers on Key Filing Dates and Key Questions.

An Introductory Video and more detailed Informational Video about the reporting requirement.

Additional guidance will be published at www.fincen.gov/boi in the coming months, to include a Small Entity Compliance Guide.

Laundering Group Suspends Russia, Publishes AML Standards, Guidance

The Financial Action Task Force (FATF), an intergovernmental body that establishes international standards for anti-money laundering, suspended Russia from its ranks, citing the Russian Federation's "actions unacceptably run counter to the FATF core principles aiming to promote security, safety, and the integrity of the global financial system."

The FATF also issued long-awaited guidance for members to implement its Recommendation 24, requiring countries to ensure that competent authorities have access to adequate, accurate and up-to-date information on the true owners of companies.

The FATF issued a public statement on February 24 at the conclusion of its plenary meeting announcing its suspension of the Russian Federation's membership from FATF.

The statement notes that "the Russian Federation's actions unacceptably run counter to the FATF core principles aiming to promote security, safety, and the integrity of the global financial system."

The FATF further urged "all jurisdictions to remain vigilant of threats to the integrity, safety and security of the international financial system arising from the Russian Federation's war against Ukraine." The FATF also reiterated "…that all jurisdictions should be alert to possible emerging risks from the circumvention of measures taken in order to protect the international financial system and take the necessary measures to mitigate these risks."

The FATF also updated its lists of jurisdictions with strategic AML/CFT/CPF deficiencies, **removing Cambodia and Morocco** from its list of Jurisdictions under Increased Monitoring and **adding South Africa and Nigeria** to the list.

The FATF's list of High-Risk Jurisdictions Subject to a Call for Action remains the same, with **Iran and the Democratic People's Republic of Korea (DPRK)** still subject to FATF's countermeasures. **Burma** remains on the list of High-Risk Jurisdictions Subject to a Call for Action and is still subject to enhanced due diligence, not countermeasures.

Reccomendation 24 Guidance

In March 2022, the FATF agreed on tougher global beneficial ownership standards in its Recommendation 24. The FATF has now updated the guidance that will help countries implement the revised Recommendation 24.

The guidance will help countries identify, design and implement appropriate measures in line with the revised Recommendation 24 to ensure that beneficial ownership information is held by a public authority or body functioning as a beneficial ownership registry, or an alternative mechanism that enables efficient access to the information.

The guidance will also help countries assess and mitigate the money laundering and terrorist financing risks associated with foreign companies to which their countries are exposed.

The guidance explains types and sources of relevant information, and mechanism and sources to obtain such information. This includes the multi-pronged approach, which consists of combining information from, among others, companies themselves, public authorities in a registry, or alternative mechanism if it ensures rapid and efficient access to beneficial ownership information. FATF's mutual evaluations demonstrated that countries using a multi-pronged approach were more effective in preventing the misuse of legal persons for criminal purposes and ensuring transparency of beneficial ownership than countries using a single approach.

The FATF Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction.

Wells Fargo Fined for Lax Sanctions Compliance

Joint action by FRB and OFAC for oversight failures

The Treasury and Federal Reserve have jointly fined Wells Fargo Bank nearly $100 million for failing to prohibit sanctions violations conducted on its trade finance platform *Eximbills* over a period of seven years.

The San Francisco Bank. agreed to pay OFAC $30 million to settle its potential civil liability for 124 apparent violations of three sanctions programs. The Federal Reserve fined Wells Fargo an additional $67.8 million for inadequate oversight.

For about seven years beginning in 2008 and ending in 2015, Wells Fargo, and its predecessor, Wachovia Bank ("Wachovia"), provided a foreign bank located in Europe with software that the foreign bank then used to process trade finance transactions with U.S.-sanctioned jurisdictions and persons.

Wells Fargo did not identify or stop the European bank's use of the software platform for trade-financetransactions involving sanctioned jurisdictions and persons for seven years despite potential concerns raised internally within Wells Fargo on multiple occasions following Wells Fargo's acquisition of Wachovia.

Wachovia specially designed a customized version of Eximbills for Bank A to "host" on Bank A's own systems, in part so that Bank A could use Eximbills to handle international trade finance instruments involving OFAC-sanctioned jurisdictions and persons. Nonetheless, Bank A's use of the Hosted Eximbills platform continued to rely on Wachovia's (and then Wells Fargo's) technology infrastructure at the bank's branch in Hong Kong and data facility in North Carolina to manage the 124 non-OFAC- compliant transactions.

A lack of clear communications within Wachovia resulted in different interpretations about whether OFAC prohibitions would be implicated by Wachovia's provision of the Hosted Eximbills platform to Bank A. Regardless, Wells Fargo's senior management should reasonably have known that Bank A was using the Hosted Eximbills platform to engage in transactions with OFAC-sanctioned jurisdictions and persons

Wells Fargo compliance and legal personnel reviewed the trade insourcing business, including by retaining a third-party consultant to review certain relevant anti-money laundering and sanctions controls. This review did not identify any sanctions compliance risks specific to the Hosted insourcing business, but one of the consultant's main conclusions was that contracts with insourcing clients contained inconsistent anti-money laundering and sanctions compliance clauses, a finding that prompted Wells Fargo to begin the process of reviewing and standardizing its insourcing contracts.

n July 2014, an internal audit report found that the insourcing business line needed corrective action because the agreements with various clients were negotiated individually, which resulted in inconsistencies. However, Wells Fargo's internal audit team did not specifically review the Hosted Eximbills platform business because **the audit team relied on the relevant business line's self-assessment that the software platform was not high risk.**

Penalty Calculation

The statutory maximum civil monetary penalty

Continues on next page

Continued from previous page

applicable in this matter is $1,066,738,422.22. OFAC determined that the Apparent Violations were voluntarily self-disclosed and that the Apparent Violations were egregious.

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 is one-half of the statutory maximum, which is $533,369,211. The settlement amount of $30,000,000 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines.

Mitigating factors:

OFAC acknowledges that, more broadly, Wells Fargo had a strong sanctions compliance program at the time of the Apparent Violations, including in the trade finance line of business, and that the failure by Wells Fargo and its senior management to identify and prevent the Apparent Violations was not a result of any systemic compliance breakdown within the broader Wells Fargo organization.

The majority of the 124 apparent violations related to agriculture, medicine, and telecommunications and therefore may have been eligible for a general or specific license, thus mitigating the harm to sanctions policy objectives.

Promptly after Wells Fargo identified the Apparent Violations, the bank terminated Bank A's access to the Hosted version of Eximbills, voluntarily disclosed the matter to OFAC, conducted an extensive internal investigation and produced the results to OFAC, and otherwise provided substantial cooperation with OFAC's investigation, including by agreeing to toll the statute of limitations

JUSTICE

Dirty Miner gets Clean Slate

A Pennsylvania coal miner formerly controlled by Texas buyout firm **Quintana Capital** has been given a pass on prosecution for FCPA violations involving $143 million in coal sales to Egypt in exchange for a $1.2 million payment to the Department of Justice Fraud Division.

TOM FISK / PEXELS

The Declination comes one year after the March 2022 arrest of **Corsa Coal** Vice President Charles Hobson. Prior to the indictment against Hobson, in November 2021, a former sales manager of the company, Frederick Cushmore, pleaded guilty to conspiracy to violate the FCPA in connection with the same scheme.

In December 2021 Quintana Capital liquidated its Corsa position by distributing its holdings of approximately 45% of the outstanding common shares of the Company to their limited partners. In 2020 and 2021 Corsa Coal had received $8.35 million in Paycheck Protection Grants from the federal government.

Corsa's attorneys successfully made the case that, despite that windfall and a record surge in coal prices, the company was able to disgorge no more than $1.2 million of the approximately $32.7 million in profits realized from the scheme.

SEC

Anglo-Australian Miner Pays $15MM to Settle Guinea Graft Case

The Securities and Exchange Commission announced charges against and a settlement with global mining and metals company, Rio Tinto plc, for violations of the Foreign Corrupt Practices Act (FCPA) arising out of a bribery scheme involving a consultant in Guinea. The company has agreed to pay a $15 million civil penalty to settle the SEC's charges.

The SEC's order finds that, in July 2011, Rio Tinto hired a French investment banker and close friend of a former senior Guinean government official as a consultant to help the company retain its mining rights in the Simandou mountain region in Guinea. The consultant began working on behalf of Rio Tinto without a written agreement defining the scope of his services or deliverables.

Eventually the mining rights were retained, and the consultant was paid $10.5 million for his services, which Rio Tinto never verified. The SEC's investigation uncovered that the consultant, acting as Rio Tinto's agent, offered and attempted to make an improper payment of at least $822,000 to a Guinean government official in connection with the consultant's efforts to help Rio Tinto retain its mining rights.

Furthermore, none of the payments to the consultant was accurately reflected in Rio Tinto's books and records, and the company failed to have sufficient internal accounting controls in place to detect or prevent the misconduct.

"Even well-designed controls need committed managers to be effective," said **Charles E. Cain, Chief of the SEC Division of Enforcement's FCPA Unit**. "Here, deficient controls were no match for managers determined to hire a consultant whose only ostensible qualification was a personal relationship with a senior government official."

Rio Tinto began exploring Simandou in the 1990s. The project controversy began after the government of now-deceased dictator Lansana Conté in 2008 stripped Rio Tinto of two of the project's four blocks, saying the miner had failed to develop the project in a timely manner.

The government awarded the rights to BSG Resources Ltd., the mining business of Israeli billionaire Beny Steinmetz, which later struck a deal with Brazil's Vale SA to buy a 51% stake in the Simandou assets.

The Guinea government later stripped BSGR and Vale of those rights, alleging they were illegally obtained. BSGR has denied any wrongdoing. Rio Tinto won the pair of blocks back in 2011, when the bribery took place.

In 2016 Rio Tinto fired Energy and Minerals Chief Executive Alan Davies and Legal and Regulatory Affairs Group Executive Debra Valentine. **The same year Rio Tinto sold its stake in Simandou to Aluminum Corp. of China for about $1.3 billion.**

OFAC

Money Transfer Company Fined for Lax Screening

Treasury's Office of Foreign Assets Control (OFAC) today announced a settlement with Uphold HQ Inc. for maintaining accounts in sanctioned countries over a five year period.

Uphold agreed to remit $72,230.32 to settle its potential civil liability for apparent violations of sanctions against Iran, Cuba, and Venezuela. Between March 2017 and May 2022, Uphold or its affiliates processed 152 transactions totaling $180,575.80 in apparent violation of OFAC's sanctions against Iran, Cuba, and Venezuela.

These apparent violations included processing transactions for customers who self-identified as being located in Iran or Cuba and for employees of the Government of Venezuela. The settlement amount reflects OFAC's determination that Uphold's apparent violations were non-egregious and voluntarily self-disclosed.

Uphold is a global multi-asset digital trading platform founded in 2014 and based in the United States. Uphold's 'Anything-to-Anything' trading experience enables customers to trade directly

Continues on next page

Continued from previous page

between asset classes with embedded payments. Customers can move, convert, and hold currency (traditional and virtual) or commodities to enable foreign exchange and cross-border remittances.

Under OFAC's Economic Sanctions Enforcement Guidelines, the base civil monetary penalty amount applicable in this matter equals the sum of one-half of the transaction value for each Apparent Violation, which is $90,288.90. The settlement amount of $72,230.32 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines.

For more information, please visit the following web notice at https://ofac.treasury.gov/media/931556/download?inline.

FBI / BIS

Montana Man TDO'd for Walkie Talkie Sale

Kenneth Scott and his company, Mission Electronics, have agreed not to engage in the export of EAR controlled material for a period of twenty years. Scott was charged in June 2022 by the U.S. Department of Commerce with violating multiple export control regulations related to the **sale of two Motorola handheld radios to Iran** with a total value of approximately $1,700.

St. Ignatius, Montana.
MARTINA NOLTE

The charges include acting with knowledge of a violation, misrepresenting and concealing facts to a U.S. government official, engaging in prohibited conduct related to the failure to file electronic export information, and failure to comply with reporting and recordkeeping requirements.

According to the charges, Scott sold, transferred, or negotiated the sale of the radios to an undercover agent, knowing that the items were destined for Iran without the required U.S. government authorization. He also failed to file electronic export information for the shipment of the radios and failed to comply with recordkeeping requirements.

In addition, Scott made false or misleading statements during interviews with FBI and BIS Special Agents, including denying that he had ever shipped anything to Iran and falsifying an email to hide his knowledge of the destination of the radios.

In responding to the BIS administrative subpoena, **Scott advised the BIS Special Agent that he has never "kept a record or a file on this stuff, as I had no idea I had to**. . . . Some of my shipping records were on my old computer that was damaged by a lightning strike about 3 years ago."

After the BIS Special Agent granted Scott additional time to respond to the subpoena, he provided some records, including a list of freight forwarders/brokers and invoices related to exports to approximately 15 countries. **For almost all of these exports, however, he failed to produce any of the other requested records, including quotes, requests for quotes, waybills, bills of lading, payment records, or emails and other correspondence.**

Mission Communications is a Reseller of New and Used Motorola equipment, including New and Reconditioned Motorola Infrastructure, located in St. Ignatius, MT (Pop. 780).

Oil Price Cap Successful, Says Treasury

'We actually do understand how commodity markets work'

The oil price cap sanctions on Russia are proving an unqualified success, according to a senior Treasury official. Speaking at the American Enterprise Institute, **Ben Harris, assistant secretary for economic policy and chief economist at the Treasury Department** discussed the price regime's effectiveness to date.

"When we announced this in the Fall we were called lots of nice things on Twitter by experts who say that you don't understand how commodity markets work you can't just cap the price of a commodity. There"ll be work arounds… We explained no we actually do understand how commodity markets work. This isn't a global price cap on a commodity, this is a conditional tweak to the sixth sanctions package, and we actually think that we have enough influence over western services that this will matter.

"We had two goals: one was to keep energy market stable and the second was to reduce Russian revenue. So here we are mid March looking back, and you say well are you successful? The first thing we'll say is look, I want to come with a lot of humility, this has only been in place for really a few weeks. February 5th is when you put in the price caps on refined product. We're not looking for a parade; things can change over time energy markets are fickle.

"That all being said we can look back at least to December 5th we put the price cap on crude and say look we had the two goals. **Prices have been remarkably stable** over the past several months and they've been trading within a band of about 7 or $8 per barrel. We've also seen Russian volumes stay relatively stable they're about where they were relative to pre war.

"The second thing you could say is OK fine barrels are flowing that's fine but you **are you driving down Russian revenue and the answer is decidedly yes.** Pre-invasion, these were basically the same product: there was about a dollar difference between the price of Brent and the price of Ural coming out of Russia. Now you're seeing a spread of about $30. What we have done is we have bifurcated the market. We've taken a commodity we've split in half. Now people care where the oil is coming from whereas before they didn't. The bifurcation in the market has allowed us to maintain this really broad spread, which ultimately drives down revenues so I think we have been successful initially

"We get the question saying look isn't this just aren't you just transferring the rents from the windfall from Russia to China or India and the answer is yes. Anyone buying cheap Russian oil is benefiting from the windfall. We are fine with it as long as it's not Russia.

"So I think I think in the short term we can we can say that this was a reasonably successful policy and we have good evidence to support that assessment. Move forward it's 2023, let's say it's 2028, 2030. What does success look like along that time horizon? **I think the most tangible measure of success is that we end the war**, and for a ton of a ton of reasons many of which are beyond the scope of my purview of the government, but this war has got to stop. I think that the price cap will not be successful until we've seen the end to the war."

Ben Harris speaking at the American Enterprise Institute

Commerce Unverified List Grows

Commerce Department's Bureau of Industry and Security (BIS) published a rule adding 32 parties in eleven countries to the Unverified List (UVL).

BIS is taking this action because it is unable to establish the bona fides – i.e., legitimacy and reliability relating to the end use or end user of items subject to the Export Administration Regulations (EAR) – of these parties for reasons outside of the U.S. Government's control.

"It is critical that BIS is able to conduct end-use checks to determine compliance with U.S. export control rules," said **Assistant Secretary Matthew S. Axelrod**. "Where we cannot verify the bona fides of foreign parties, we will continue to add parties to the Unverified List to place restrictions on future export transactions and prevent the diversion of U.S. items."

Failure to establish an entity's bona fides, which may include an inability to contact or locate the party, failure by the party to appropriately demonstrate the disposition of items subject to the EAR, or lack of cooperation by a host government with BIS's conduct of end-use checks.

Listing on the UVL does not mean that exporters cannot engage with listed parties. However, transactions with parties on the UVL require, among other things, additional documentation, including a statement from authorized officials of listed parties, and such transactions are not eligible for authorization pursuant to EAR license exceptions.

The UVL (supplement no. 6 to part 744) is one of several lists, including the Entity List (supplement no. 4 to part 744) and the Military End User List (supplement no. 7 to part 744), administered and maintained by BIS. These lists inform exporters and the general public of end-users that are of concern for various reasons, and that are subject to specific requirements or prohibitions in the EAR.

The entities are located in: Bulgaria, Canada, Indonesia, Israel, Malaysia, Saudi Arabia, Singapore, the People's Republic of China (14), Germany (2), Turkey (4), and the United Arab Emirates (5). The text of the rule, which is effective upon publication and includes the names of the entities added to the UVL, is available at https://public-inspection.federalregister.gov/2023-06171.pdf

---

UAV

Sixth Iran Aerospace Sanction Block

The Treasury Department is designating a network of five companies and one individual for supporting Iran's unmanned aerial vehicle (UAV) procurement efforts.

The China-based network is responsible for the sale and shipment of thousands of aerospace components, including components that can be used for UAV applications, to the Iran Aircraft Manufacturing Industrial Company (HESA). HESA has been involved in the production of the Shahed-136 UAV model that Iran has used to attack oil tankers and has exported to Russia.

"Iran is directly implicated in the Ukrainian civilian casualties that result from Russia's use of Iranian UAVs in Ukraine," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "The United States will continue to target global Iranian procurement networks that supply Russia with deadly UAVs for use in its illegal war in Ukraine."

OFAC's actions are taken pursuant to E.O. 13382, which targets weapons of mass destruction proliferators and their supporters. Since September 2022, the United States has issued six rounds of designations of individuals and entities involved in the production and transfer of Iranian UAVs.

"Iran cultivates complex sanctions evasion networks where foreign buyers, exchange houses, and dozens of front companies cooperatively help sanctioned Iranian companies to continue to trade," said Deputy Secretary of the Treasury Wally Adeyemo. "Today's action demonstrates the United States' commitment to enforcing our sanctions and our ability to disrupt Iran's foreign financial networks, which it uses to launder funds."

OFAC

More Iran Drone Actions

Treasury's Office of Foreign Assets Control (OFAC) designated four entities and three individuals in Iran and Turkey for their involvement in the procurement of equipment, including European-origin engines of unmanned aerial vehicles (UAV) in support of Iran's UAV and weapons programs.

This procurement network operates on behalf of Iran's Ministry of Defense and Armed Forces Logistics (MODAFL), which oversees several firms involved in UAV and ballistic missile development.

Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "The United States will continue to expose foreign procurement networks in any jurisdiction that supports Iran's military industrial complex."

Today's action, which follows OFAC's March 9, 2023 designation of a China-based network in connection with Iran's UAV procurement efforts, as well as several previous OFAC actions targeting Iran's UAV manufacturers and their executives since September 2022, is being taken pursuant to Executive Order (E.O.) 13382.

MODAFL was designated pursuant to E.O. 13382 on October 25, 2007, for having engaged, or attempted to engage, in activities or transactions that have materially contributed to, or pose a risk of materially contributing to, the proliferation of weapons of mass destruction or their means of delivery. E.O. 13382 targets weapons of mass destruction proliferators and their supporters

Related Indictments

A federal court in the District of Columbia unsealed two indictments Tuesday charging multiple defendants with violations of the Arms Export Control Act (AECA) and the International Emergency Economic Powers Act (IEEPA) for their roles in separate schemes to procure and export U.S. technology to Iran between 2005 and 2013.

One indictment concerned the export from the United States and transshipped through Turkey a device that can test the efficacy and power of fuel cells and attempted to obtain a bio-detection system that has application in weapons of mass destruction (WMD) research and use.

The second case charged conspiracy to obtain U.S. technology, including a high-speed camera that has known nuclear and ballistic missile testing applications, a nose landing gear assembly for an F-5 fighter jet, and a meteorological sensor system. Justice release: https://www.justice.gov/opa/pr/justice-department-announces-charges-and-sentence-connection-iranian-procurement-network-s

State Expands Paraguay Corruption Sanctions

The State Departement designated of the former Director of the Paraguayan Civil Aviation Authority, a current member of the Paraguayan Panel for the Discipline of Judges and Prosecutors and current Court Clerk Vicente Ferreira for "their involvement in significant corruption."

AP Reports that Paraguay's attorney general launched a criminal investigation Thursday into U.S. allegations that a former Paraguayan president Horacio Cartes and the current vice president were involved in corruption and had ties to a terrorist group.

The U.S. asserts the porous border region that connects Argentina, Bolivia, Brazil and Paraguay is a hub for money laundering of illicit activity.

In January the State Department issued sanctions against former President and current Vice, citing "systemic corruption that has undermined democratic institutions in Paraguay."

The State Department has said that corruption in Paraguay often prevents convictions in money-laundering and terrorism financing cases.

OFAC

Sanctions Don't Relieve Settlement Obligations

Treasury's Office of Foreign Assets Control (OFAC) issued a license permitting a sanctioned Paraguayan tobacco company to continue its remittances under the 1998 Tobacco Master Settlement Agreement.

General License No. 7, issued under Global Magnitsky Sanctions Regulations 31 CFR part 583

Authorizing Certain Transactions Involving Tabacalera del Este S.A. or Tabacos USA Inc. Pursuant to the 1998 Tobacco Master Settlement Agreement

Continues on next page

Continued from previous page

Transactions that are ordinarily incident and necessary to payments under the tobacco Master Settlement Agreement (MSA), entered into on November 23, 1998 between certain U.S. state and territory attorneys general and certain tobacco companies, are authorized.

On January 26, 2023, OFAC designated former Paraguayan president Horacio Manuel Cartes Jara (Cartes) pursuant to Executive Order 13818 for involvement in corruption and also designated Tabacos for being owned or controlled by Cartes.

On March 31, 2023, OFAC identified Tabesa as an entity that is owned, directly or indirectly, 50 percent or more by Cartes and added Tabesa to the SDN List.

Global Magnitsky General License 7 does not authorize debits to any blocked account on the books of a U.S. financial institution or any other transactions otherwise prohibited by the Global Magnitsky Sanctions Regulations.

OFAC

Assad Cronies Named Drug Traffickers

Treasury's Office of Foreign Assets Control (OFAC) and UK officials namedassociates of Syrian President Bashar al-Assad for the production or export of Captagon, a dangerous amphetamine.

The trade in Captagon is estimated to have become a billion-dollar illicit enterprise. These designations, some of which are being implemented pursuant to the Caesar Syrian Civilian Protection Act of 2019 ("Caesar Act"), also highlight the important role of Lebanese drug traffickers — some of whom maintain ties to Hizballah — in facilitating the export of Captagon. This action also underscores the al-Assad family dominance of illicit Captagon trafficking and its funding for the oppressive Syrian regime.

"Syria has become a global leader in the production of highly addictive Captagon, much of which is trafficked through Lebanon," said OFAC Director Andrea M. Gacki. "With our allies, we will hold accountable those who support Bashar al-Assad's regime with illicit drug revenue and other financial means that enable the regime's continued repression of the Syrian people."

Allies Finally Budge on Russian Conflict Diamonds

Following through on their commitment to "work collectively on further measures on Russian diamonds," made after last month's G-7 Summit, US and European Commission officials met March 6th to discuss with representatives of leading diamond retailers, manufacturers, laboratories, and industry trade associations future Russia-related import measures.

Russia continues to earn billions of dollars from the diamond trade, and the discussion centered on the most effective and impactful ways to disrupt that revenue stream. Progress has been impeded by resistance from the Belgian government, which has now ended.

"Russian diamonds are blood diamonds," Prime Minister Alexander De Croo said in a statement to *Politico*."The revenue for Russia from diamonds can only stop if the access of Russian diamonds to Western markets is no longer possible. On forging that solid front, Belgium is working with its partners."

US, but not European sanctions target Russia's Alrosa, the world's largest diamond mining company, responsible for 90 percent of Russia's diamond mining capacity and accounting for 28%, or nearly a third, of global diamond output.

OFAC

Updates Burma & Belarus Sanctions

Treasury's Office of Foreign Assets Control (OFAC) is amending and reissuing the **Belarus Sanctions Regulations** to implement an August 9, 2021 Belarus-related Executive Order and incorporate a directive regarding sovereign debt.

OFAC is also publishing an alert regarding sanctions on jet fuel sales to the Burmese military. For additional information about risks associated with doing business with Burma's military regime.

RAPTAC

Regulations & Procedures Roundup

The Commerce Department's Bureau of Industry and Security Regulations and Procedures Technical Advisory Committee held a marathon open session Tuesday, with a particular emphasis on the microelectronics supply chain.

Sharron Cook, of the BIS Regulatory Policy Division began with an update on the October 7th Advanced Computing and Semiconductor Manufacturing Equipment Rule. Comments were due January 31st, with the final rule pending interagency review. No date is available for publication of the final rule, though an updated FAQ is in review and will be available "shortly."

"Always look at your red flags, audit your supply chains to the extent possible, to identify in the US origin inputs in the production of the items, and obtain confirmation from suppliers regarding the origin of parts and components," said Ms. Cook. "And as always, keep good records to back up your analysis of the transactions."

Next up, a team from the **Strategic Radiation Hardened Electronics Council** discussed collaborative efforts across agencies and industry to ensure survivable electronics, terrestrial and in space.

The SHREC Initiative, begun in 2018, is "important as we're modernizing all of our nuclear weapons programs, space programs and missile defense program. Most of the technology that we have in our legacy systems is based on 150 nanometer node technology which is early 90s technology, so state-of-the-art technology is something that we're interested in doing now.

"Radiation hardened microelectronics for Department of Defense is a niche within a niche within a niche, so we have very small demand. Really only the US government DoD has those requirements, so it's really hard to get state-of-the-art technologies based on our demand. It's hard for the companies to make money when they only have so many wafers."

Researchers are discovering what can be referred to as **"radiation hardened by serendipity, where properties of circuits li the very low nanometer sizes** (14 and below) are increasingly being discovered through testing as having very attractive talents, or even hardened properties. This is coming off the standard commercial manufacturing processes."

Other speakers included **Evan Broderick Acting Executive Director for the Information and Communications Technology and Services** program at BIS, an update on Enforcement from Kevin Kurland, Deputy Assistant Secretary for Export Enforcement, Charles Wall, BIS Senior Policy Advisor on the US-EU Trade and Technology Council and Matthew Borman, Deputy Assistant Secretary of Commerce for Export Administration.

'If it can communicate, we can regulate it'

Chief of OICTS discusses new export regulator

Evan Broderick, Acting Executive Director *of the Information and Communications Technology and Services (ICTS)* program at BIS, discussed the OICTS, a rapidly growing enforcement activity that set up shop last March.

Broderick

Mr. Broderick manages operations and policy development under Executive Orders 13873, 14034, and 13984. His comments were delivered during a presentation to the Regulations and Procedures Technical Advisory Committee (RAPTAC) March 21st.

"The program started with the 2019 Order 13873. That is **the Supply Chain EO** as it's commonly referred to. It is essentially said that the secretary of commerce can prohibit or mitigate ICTS transactions: information and communications technology transactions that used data in transferred from and linked to a foreign adversary.

Continues on next page

Continued from previous page

"Essentially it's anything that can communicate, that touches the Internet. We're talking telecom, satellites, mobile phones, and the WeChat TikTok issue. It's also 5G equipment, it's cyber security, software, it's cloud. If it if it can communicate, then we can regulate it.

"We do have investigations into multiple Chinese companies here in the US . The secretary announced that in March of last year. We have not yet taken any public action on them so you did not miss anything.

"Right now we have less than 10 people within the organization, and we have asked for and received $27 million from Congress as of this January. We have requested 100 full-time employees or full-time equivalent and we received that. Now, when it comes down to it though, it's going to take some time to ramp up the resources."

Different from CFIUS

Stephen Mulligan with the Congressional Research Service points out the following:

"Some observers have likened the ICTS review process to CFIUS, which assists the President in overseeing the national security implications of foreign investment in the U.S. economy. Both CFIUS and the ICTS review involve interagency processes to review and block certain commercial transactions with foreign entities that present national security concerns.

"However, while CFIUS traditionally reviews major corporate restructurings and acquisitions, the **Supply Chain Rule authorizes Commerce to review individual commercial sales.**

"For example, whereas CFIUS might prevent a foreign entity from acquiring a stake in a U.S. semiconductor company, under the Supply Chain Rule, Commerce could block a U.S. company from buying individual semiconductors from a foreign company in a foreign adversary's jurisdiction"

Call for Industry Cooperation in Arms Tracing

NGO mapping supply chains in Ukraine ask for help.

The RAPTAC received a briefing by Damien Spleeters, Conflict Armament Research, on chains of supply of components found in Russian and Iranian weapons used in Ukraine, and his organizations outreach to industry.

CAR is an independent research organization that is investigating the diversion of weapons and commodities in conflict areas around the world, funded by the EU and the US government. CAR investigation teams work on the ground in active armed conflicts. The teams document weapons at the point of use and track their sources back through the chains of supply.

"We have a pretty thorough tracing process, in which we will send a what we call a 'trace request' to the manufacturers with all the markings, all the photos, all the contextual information that we have gathered. We give them 28 days for a response.

"Then we we will in general we will discuss with manufacturers information sharing protocols and what they are ready to share with us. Once they respond, we give them what we call a 'right of reply.' We will summarize all the information they have provided to us into a text for them to comment or correct if they'd like to, and we give them another 28 days to do that.

Hembo Pagi, (CC BY-NC 2.0)

"So all the entities we contact are aware of the information that we can use, and they are in control of that. There's there's no surprise when we use that information to update the EU the US or to continue our own investigations.

"The entities we have engaged with so far have been very happy with how it went and as I said we are we are flexible in the way that we use the information. We always agree with the manufacturer or with the entity on what is going to happen with the information they give us.

"In some cases they're happy for us to receive information for us to continue the investigation, but they don't want some of the distributors to be named publicly, for example. We are happy to accommodate that type of demand because the last thing we want to do is hurt business."

CBP Forced Labor Expo Gets Schooled

'Everyone needs to be looking'

In a presentation the CBPs Forced Labor Expo in Wednesday, **Dr. Laura Murphy of Sheffield Hallam University** (UK) made an impassioned plea for industry to know their supply chain.

[Her comments have been edited for brevity.]

"What we're talking about here today is extraordinarily urgent. It is probably, I hope, the worst human rights crisis we'll see in our lifetimes. Our team have traced the ways in which the Chinese government the PRC government has invested enormous resources in moving manufacturing to the Uyghur region intentionally, to transform that region. **Transforming that region they claim is a development project, but it is in fact a major integral part of a genocide.**

We look at how that forced labor is affecting our international supply chains and try to produce the knowledge base that allows us to take action. We've looked at solar we've looked at cotton apparel we've done research on PVC and building materials, and we looked at the automotive industry.

The thing that I think might be being missed here is that when folks talk about labor transfers that is a euphemism. It's a neat clean phrasing for a system of forced labor. The way we know that is because, while labor transfers and operate across the entirety of China, in the Uyghur region they operate on a backdrop of extraordinary coercion that is that is mechanized that is operationalized through the threat of internment.

The thing about the situation in the Uyghur region is those labor transfers - somebody could say yes to them, but no one can say no. To resist a government program is to be aligned with terrorism; this is directly written into government directives. Anyone who says no knows that they are risking going to an internment camp, and they know what happens there because there is no one in that region who has not gone, or been, or had a family member go to a camp.

Murphy

There are few things that experts in the world agree on but experts on forced labor agree on: this system is a massive and unprecedented system of state sponsored forced labor, and so it is all of our duty to address.

People told us the Xinjiang region is a black box, but the truth is if we can see it you can see it. It is all online. We are not hackers; we don't know anything about the dark web. We just Google it y'all. We Google it in Chinese. You could use Google Translate.

So if we can see it you can see it. You can be doing this work. You can use these tools, but you could also just Google your suppliers name in Chinese. I cannot tell you how many companies tell me they do not know their supplier's Chinese name. How do you know anything about your supplier if you don't even know what their name is, right?

We trace supply chains out to the rest of the world and what we're finding is that **companies and whole industries have remained ignorant of their raw materials.** We go as far as we can down into the raw materials. We look at companies that are egregiously engaged in the labor transfer programs. We document what they've done, and we then say OK who are they selling to?

China has decided that they're going to move the dirty processing of the actual raw materials to the Uyghur region — where they don't care what happens to the environment, where processes that are outlawed all over the world, including in other parts of China are still being practiced in the Uyghur region with complete impunity.

What we found was that everyone needs to be looking if you have any raw materials that are that could possibly be processed in China they're moving to that region and you need to be looking at your supply chains to figure that out. We have the opportunity to do the right thing and say we're not going to just not buy those goods for the

I regularly hear from businesses about the risk. We need to, you know, limit our risk, our exposure. We need to limit our financial risk, our legal risk. As a human rights researcher, I think you're talking about the wrong risk.

There are 12 million people in the Uyghur region. 12 million people who every single day are terrified that they will have a sack put over their heads, that they will disappear in the night. People who go to sleep wearing layers of clothes so that when they end up in an internment camp they have underwear.

Three million Uyghur workers work for you. You may not pay them directly; no one pays them directly. You are profiting from them, and you are talking about your business risk, your legal risk.

I am talking about the risk of participating in a genocide, of financing

Continues on next page

Continued from previous page

a genocide, because that's what we're doing, and consumers can only do so much to prevent that. I can only do so much wearing of my used clothes to be able to prevent that.

So I don"t want to hear talking about risk to your business, I like talking about risk to Uyghur people, and until you are doing every single thing you can do to make sure that you change what's happening for the Uyghur people, or at least make sure that you're not profiting from it, you're doing every single thing you can do, you should not sleep at night. I mean it.

For all of that said I think there's some reasons for us to be optimistic. I think that we have together done some pretty incredible things to address this crisis. It's remarkable as someone who lived in the Uyghur region, who's watched this situation deteriorate over 20 years, to see how people have come together and how quickly we've been able to make change when people finally recognized how urgent this situation is.

Laura T. Murphy is Professor of Human Rights and Contemporary Slavery at the Helena Kennedy Centre for International Justice at Sheffield Hallam University (UK).

CBP Uyghur Enforcement Picks Up

Our friends at Sandler Travis & Rosenberg report CBP is now detaining PVC products such as vinyl flooring under the UFLPA and asking importers to trace these items back to their originating chemicals such as chlorine, carbon, and ethylene.

While the UFLPA specifies tomatoes, cotton and polysilicon as high-priority sectors for UFLPA enforcement, according to detention notices CBP issues with regard to potentially violative goods, PVC has been added as a sector of concern after aluminum was added in October 2022.

A June 2022 report published by UK's Sherffield Hallam University and Maine's Materials Research notes that the top export application for China-originating PVC is luxury vinyl floor coverings. PVC flooring resins made in China are present in more than one-quarter of all flooring sold in the U.S.

- The two largest PVC manufacturers in China are both state-owned enterprises based in the XUAR
- All of the Uyghur Region's PVC companies have been active participants in the XUAR's notorious labour transfer programs.

Those companies export to 73 intermediary manufacturers, who then export PVC-based building materials to at least 158 companies worldwide. Brands selling flooring at very high risk of Xinjiang inputs include Home Legend for Home Depot, Armstrong, Mannington Mills, Mohawk, Lumber Liquidators, Congoleum, and many others.

CBP Outreach Efforts

CBP is undertaking multiple efforts to provide more information for companies seeking to comply with the Uyghur Forced Labor Prevention Act and Section 307 of the Tariff Act of 1930 (19 U.S.C. 1307).

On **February 23, 2023,** CBP released additional guidance on enforcement and review procedures under the Uyghur Forced Labor Prevention Act:

- More detailed FAQs
- Best Practices for Applicability Reviews
- Guidance on Executive Summaries and a Sample Table of Contents

On **March 14-15, 2023**, CBP's Office of Trade will host the Forced Labor Technical Expo in Washington D.C. The Forced Labor Technical Expo will offer a forum for industry to provide the international trade community with information about the latest technologies that can aid in securing and managing the flow of goods. Register at www.cbp.gov/trade/forced-labor.

ACE Updates for UFLPA

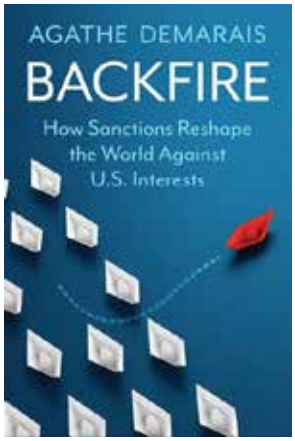
On **March 18, 2023**, CBP will deploy the Uyghur Forced Labor Prevention Act (UFLPA) Region Alert enhancement to the Automated Commercial Environment (ACE). This enhancement will provide an early notification to importers and their representative of goods that may have been produced in the Xinjiang Uyghur Autonomous Region (Xinjiang or XUAR) and may be excluded from importation into the United States. This enhancement includes electronic data interchange (EDI) impacts.

The UFLPA was signed into law on December 23, 2021 (Public Law 117-78) and implemented on June 21, 2022. It supports U.S. Customs and Border Protection's (CBP) forced labor enforcement authorities and establishes a rebuttable presumption that all goods, wares, articles, and merchandise mined, produced, or manufactured wholly or in part in the Xinjiang region of the People's Republic of China, or by entities identified by the United States government on a UFLPA entities list, are prohibited from entry in the United States.

Backfire:

How Sanctions Reshape the World Against U.S. Interests

In "Backfire," by **Agathe Demarais,** Columbia University Press, critically examines the effectiveness and long-term viability of sanctions as a policy tool for coercion. She argues that, despite a few high-profile successes, sanctions often fail to influence targeted states and can trigger backlash, undermining their effectiveness.



Demarais, an economic forecaster and former member of the French foreign service, writes from an industry perspective, offering insights into how firms interact with sanctions.

She presents two strong case studies: the Nord Stream II situation and the Rusal designation case, illustrating the unpredictability of sanctioning institutions integrated into the global supply chain.

The book highlights the limitations and negative side effects of sanctions, such as humanitarian consequences, compliance difficulties for banks and firms, and potential harm to the countries imposing them.

Full of counterintuitive insights spanning a wide range of topics, from Russia's invasion of Ukraine to Iran's COVID response and China's cryptocurrency ambitions, the book reveals how sanctions are transforming geopolitics and the global economy—as well as diminishing U.S. influence.

"Backfire" provides an eye-opening, accessible, and timely account that sheds light on the future of sanctions in an increasingly multipolar world.

In a February article in *Foreign Policy*, Desmarias entered the debate on the effectiveness of the Allied sanctions campaign against Russia, positing six lessons learned and four questions for the future:

• **Sanctions are no magic bullet**: While they can constrain Russia's war efforts, they won't produce regime change, cause economic collapse, or alter the Kremlin's calculus.

• **Sanctions need clear objectives**: Clearly defined goals help avoid confusion and increase the likelihood of achieving results.

• **Western unity on sanctions has been faultless**: Trans-Atlantic unity on sanctions has been strong, defying Putin's expectations of disunity.

• **Chinese firms are not rushing to Russia**: Chinese businesses haven't flocked to fill the void left by Western sanctions, maintaining a relatively stable trade relationship.

• **Russia manipulates statistics**: The Kremlin uses data as a tool in its disinformation war, spreading doubt about the impact of sanctions.

• **Sanctions are biting, but recovery will be slow**: While Russia's economy didn't contract as much as predicted, it will take years to return to prewar levels.

What comes next depends on addressing four key questions:

• Can the West tighten sanctions implementation and close loopholes?

• Can Russia's sanctions propaganda in the global south be countered?

• Will the United States impose secondary sanctions on Russia?

• How can the West tackle sanctions resistance?

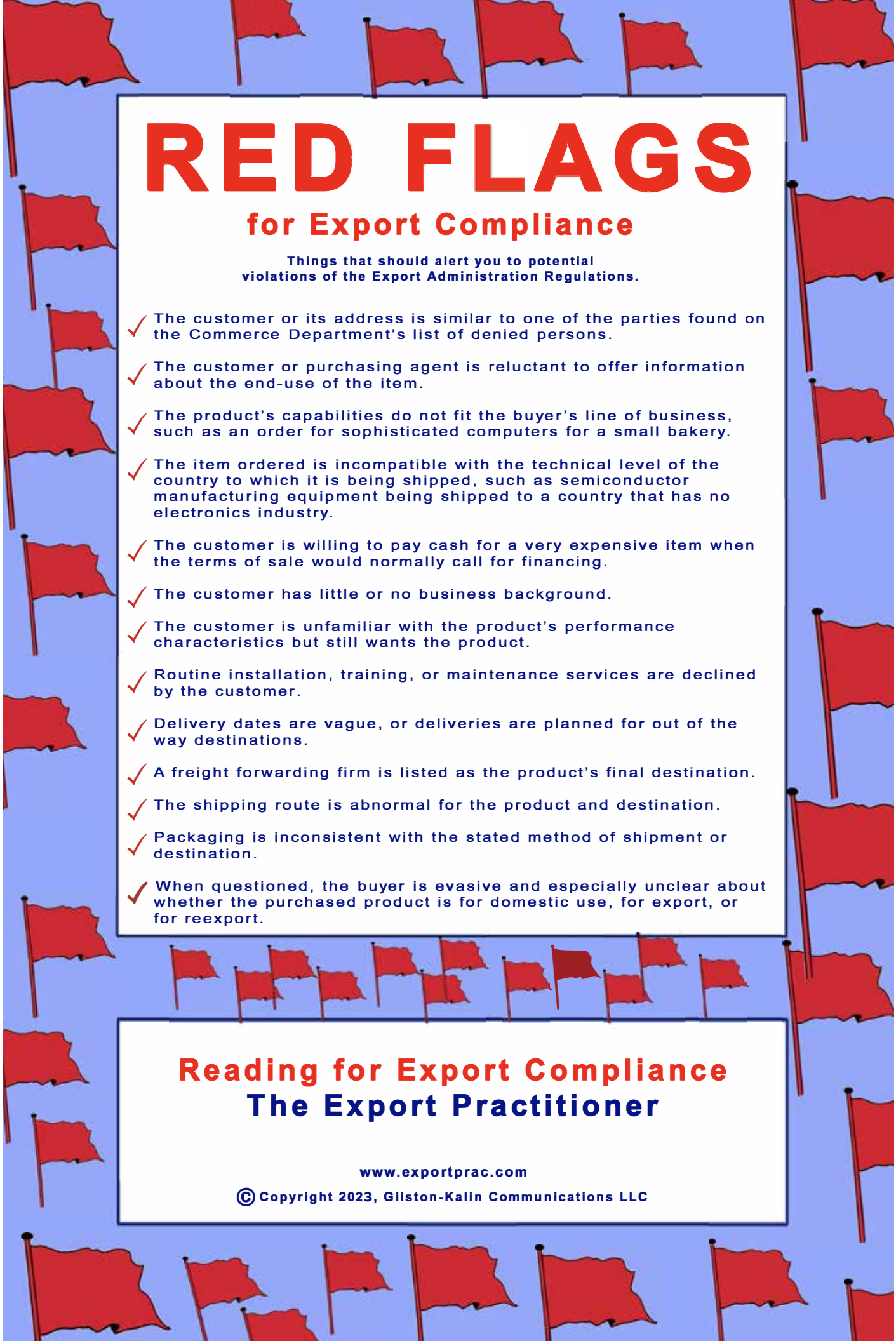
SIPRI Arms Trade Report

This month the Stockholm International Peace Research Institute (SIPRI) released their annual update on international arms transfers.

The data revealed that imports of major arms by European states increased by 47 per cent between 2013–17 and 2018–22, while the global level of international arms transfers decreased by 5.1 per cent. Arms imports fell overall in Africa (–40 per cent), the Americas (–21 per cent), Asia and Oceania (–7.5 per cent) and the Middle East (–8.8 per cent)—but imports to East Asia and certain states in other areas of high geopolitical tension rose sharply.

The United States' share of global arms exports increased from 33 to 40 per cent while Russia's fell from 22 to 16 per cent.

"Even as arms transfers have declined globally, those to Europe have risen sharply due to the tensions between Russia and most other European states,' said **Pieter D. Wezeman**, Senior Researcher with the SIPRI Arms Transfers Program.



RED FLAGS

for Export Compliance

Things that should alert you to potential violations of the Export Administration Regulations.

- ✓ The customer or its address is similar to one of the parties found on the Commerce Department's list of denied persons.
- ✓ The customer or purchasing agent is reluctant to offer information about the end-use of the item.
- ✓ The product's capabilities do not fit the buyer's line of business, such as an order for sophisticated computers for a small bakery.
- ✓ The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- ✓ The customer is willing to pay cash for a very expensive item when the terms of sale would normally call for financing.
- ✓ The customer has little or no business background.
- ✓ The customer is unfamiliar with the product's performance characteristics but still wants the product.
- ✓ Routine installation, training, or maintenance services are declined by the customer.
- ✓ Delivery dates are vague, or deliveries are planned for out of the way destinations.
- ✓ A freight forwarding firm is listed as the product's final destination.
- ✓ The shipping route is abnormal for the product and destination.
- ✓ Packaging is inconsistent with the stated method of shipment or destination.
- ✓ When questioned, the buyer is evasive and especially unclear about whether the purchased product is for domestic use, for export, or for reexport.

Reading for Export Compliance
The Export Practitioner

www.exportprac.com