

EP

IN THIS ISSUE:

- AUKUS: State Patch 'til NDAA
- UC Berkeley Scolded for China
- EXIM backs Swiss Hedge Fund
- Voluntary Self-Disclosure Guidance

THE EXPORT PRACTITIONER™



Open Source Software and Export Control

Navigating Risks for Global Collaborative Development

WELCOME TO YOUR NEW EXPORT PRACTITIONER™ IN PRINT | VIA EMAIL | ONLINE

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.

Link to Our
Top Stories:



**TO SUBSCRIBE,
OR TO SUBMIT CONTENT:**

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

VISIT ONLINE AT
EXPORTPRAC.COM



EP

THE EXPORT PRACTITIONER™

August 2023 | VOL. 37, NO. 8

FEATURE

Open Source Software and Export Control

• Navigating Risks for Global Collaborative Development | 4



ELCHINATOR/PIXABAY

POLICY

AUKUS Tech Update: ATAM, NDAA, ITAR Waivers | 7

U.Cal Berkeley: China Collaboration Targeted | 9

Data Privacy: EU - U.S. Data Privacy Framework | 11

CAPITAL

CFIUS: Treasury Releases Annual Report | 12

CFIUS: House Bill to Include Land Purchases | 12

EXIM: Hedge Fund, Looser Terms, Solar Billions | 15

EXPORT CONTROLS

Raimondo on More China Controls | 16

BIS: Licensing for Medical-Related Items | 17

State: Myth & Fact on Export Controls | 18

SANCTIONS

Voluntary Self Disclosure: Tri-Shield Note | 19

OFAC: Russia Sanctions Heavied Up | 19

ENFORCEMENT

OFAC: Video Series, Gacki Departs | 21

Antiboycott: Contractors Settle Charges | 22

Briefs: Deutsche Bank, S. Korea, Balkans | 23

SUPPLY CHAIN

UFLPA: FTETF Update, Solar Compliance | 24

Ford Motor EV Sourcing Criticized | 26

Briefs: Defense Industrial Base, Cattle Laundering | 27

ON THE COVER: Developers can modify and adapt FOSS software to meet their specific needs. MARKUS SPISKE

The Export Practitioner

www.exportprac.com

Mailing Address: P.O. Box 7592, Arlington, VA 22207

Telephone: 703-283-5220

E-Mail: info@traderegs.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.

Copyright 2023 Gilston-Kalin Communications, LLC
ISSN 1087-478K



ADOBE STOCK

Open Source Software and Export Control

Navigating Risks for Global Collaborative Development

By **DAVE HARRIS**
TC Engine

Free and Open Source Software (FOSS) refers to software that is released with a license that grants users the freedom to use, modify, and distribute the software. It is built on the principles of collaboration, transparency, and community-driven development.

The value of FOSS is manifold. It promotes collaboration and knowledge sharing among developers, enabling them to access and build upon existing software solutions. FOSS encourages

innovation, as developers can modify and adapt the software to meet their specific needs. The transparent nature of FOSS allows for thorough code review, enhancing software security and reliability.

Additionally, FOSS often benefits from a vibrant community of contributors who provide support, updates, and improvements, leading to faster development cycles and increased stability.

FOSS provides numerous benefits for developers, including collaborative development, flexibility, and the ability to leverage existing solutions. However, it also requires careful license compliance, intellectual property considerations, security awareness, community

evaluation, integration management and as you will come to understand, unique Trade Control challenges.

FOSS License Types of Trade Control rules (or lack thereof)

While there are over 50 examples, we find three dominant types of FOSS licensing:

GNU GENERAL PUBLIC LICENSE (GPL):

The GNU GPL is one of the most well-known and widely used FOSS licenses. It was created by Richard Stallman and the Free Software Foundation (FSF) in the 1980s.

From a Trade Control perspective, the GPL does not explicitly include provisions for export control or restrict the sharing of software across borders. This lack of specific Trade Control measures means that companies collaborating globally using GPL-licensed software may face risks related to compliance with international trade regulations.

If the software contains export-controlled technology or data, companies need to ensure that its sharing and distribution comply with applicable export control laws.

APACHE LICENSE:

The Apache License is known for being business-friendly and permissive, allowing users to modify, distribute, and sublicense the software under certain conditions.

Similar to the GPL, the Apache License does not specifically address Trade Control requirements or export control considerations. This lack of explicit Trade Control provisions introduces potential risks for companies engaged in global collaboration using Apache-licensed software. Companies must ensure that the software and any export-controlled components or technologies comply with the applicable trade regulations of the jurisdictions involved.

MIT LICENSE:

The MIT License is a permissive FOSS license widely used for many software projects. It is known for its simplicity and flexibility. The MIT License allows users to use, modify, and distribute the software under certain conditions, while disclaiming warranties and liability.

As with the other licenses mentioned, the MIT License does not include specific Trade Control

provisions or address export control requirements. Companies utilizing MIT-licensed software for global collaboration need to be aware of the potential risks related to export-controlled technology or data. It is essential for organizations to evaluate and address any Trade Control obligations associated with the software they use, particularly when collaborating across international borders.

Overall, the risk introduced by the use of FOSS licenses without explicit Trade Control provisions lies in the potential violation of export control regulations. Companies must ensure that their collaboration and distribution of FOSS comply with the applicable Trade Control laws of the jurisdictions involved, especially when dealing with export-controlled encryption, technology or data.

Failure to do so can result in severe legal and regulatory consequences, including fines, loss of export privileges, and damage to a company's reputation. It is crucial for organizations to have proper trade compliance mechanisms in place when utilizing FOSS for global collaborative development.

Focus on encryption

The use and expansion of encryption in FOSS development can introduce Trade Control risks, particularly concerning the export and import of cryptographic technology.

OPENSSL:

OpenSSL is a widely used FOSS library that provides encryption, cryptographic, and SSL/TLS functionalities. It offers a robust set of encryption algorithms, such as AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and others.

GNUPG (GNU PRIVACY GUARD):

GnuPG, also known as GPG, is a FOSS implementation of the OpenPGP standard, providing

Continues on next page

Overall, the risk introduced by the use of FOSS licenses without explicit Trade Control provisions lies in the potential violation of export control regulations.

Continued from previous page

encryption and digital signature capabilities. It allows users to encrypt and decrypt messages, verify digital signatures, and manage key pairs.

LIBSODIUM:

libsodium is a modern and easy-to-use FOSS library for encryption, decryption, signatures, password hashing, and more. It aims to provide a high-level and secure interface for developers. libsodium includes encryption algorithms like XSalsa20, XChaCha20, and AEAD (Authenticated Encryption with Associated Data) constructions like ChaCha20-Poly1305.

It's important for companies engaged in FOSS development, particularly in a global collaborative context, to understand the Trade Control risks associated with encryption technologies. Software developers should collaborate with their Trade Control or legal experts and develop a Playbook to stay informed about the export control requirements of the jurisdictions involved to mitigate Trade Control risks effectively.

What are the rules related to 'export' when it comes to FOSS?

Under the U.S. Export Administration Regulations (EAR), there is an exemption known as the "publicly available" rule (EAR §734.3(b)(3)). This rule allows for the release of certain technology, including encryption software, without requiring an export license, provided it meets specific criteria.

According to the "publicly available" rule, technology is considered publicly available if it has been published or made available to the public without any restrictions on access or dissemination. The rule covers technology that is generally accessible to the public, such as through open source software distributions, public repositories, or public websites.

While the "publicly available" rule applies under U.S. export control law, it is important to note that the same exemption may not apply in other jurisdictions, including Australia (AU), Canada (CA), and the United Kingdom (UK). Each country has its own export control regulations and may have different criteria and requirements for determining what constitutes "publicly available" technology.

What are the potential risks and implications when a company circumvents the direct download of FOSS from a publicly available source repository?

Under the "publicly available" rule, technology is considered publicly available if it is made accessible to the public without restrictions on access or dissemination. By downloading FOSS directly from a publicly available source repository, companies can take advantage of the exemption without the need for an export license.

However, when a company modifies the FOSS source code or distributes it from an internal server, these modifications or restrictions on access could affect the determination of whether the technology remains publicly available or not.

To mitigate these risks and ensure compliance, companies must exercise diligence and understand the potential implications of modifying FOSS source code or distributing it from internal servers.

It is crucial for companies to have clear policies and procedures in place to manage their FOSS usage, including tracking modifications, understanding the implications of those modifications on export control requirements, and maintaining proper documentation.

By doing so, companies can ensure they are compliant with relevant export control regulations and avoid potential penalties or legal consequences.

David Harris is a Partner of TC Engine providing software solutions that automate trade compliance processes, reduce the risk of non-compliance, and meet regulatory requirements. www.TCEngine.com (253) 495-7974. dave.harris@tcengine.com

Scan the code below for a broader discussion of definitions, considerations and jurisdictional classification or go to:

https://www.exportprac.com/detail.html?sub_id=4fdf3a748d



AUKUS Tech Pact Update

THE STATE DEPARTMENT has published a Memo articulating the **AUKUS Trade Authorization Mechanism (ATAM)** designed to facilitate trade of U.S. defense articles and defense services between the United States, the UK, and Australia in support of AUKUS programs.

The AUKUS pact, a defense agreement among Australia, the United States, and Britain, was signed in 2021 and involves \$368 billion worth of investments.

The transfer of submarines to Australia is a key part of the agreement, aimed at bolstering the Indo-Pacific region's security in the face of challenges from China.

AUKUS involves changes to U.S. export controls related to **Pillar I** (providing Australia with a conventionally armed, nuclear-powered submarine capability) as well as **Pillar II** (advanced capabilities, including hypersonic ballistics.).

The State action is an interim measure to streamline defense trade of U.S. origin items while the administration pursues legislative changes.

The AUKUS Trade Authorization Mechanism will provide a consistent framework that will cover **Direct Commercial Sales (DCS)** (private sector-to-government or private sector-to-private sector transfers) as well as some items that were previously sold as **Foreign Military Sales (FMS)** (government-to-government agreements) but may be handled as DCS under ATAM.

This mechanism relies on existing authorities, both to increase the speed and efficiency of defense trade while doing so in a way that is familiar, and therefore easier, for U.S. exporters.

This approach was adopted to address concerns regarding how the speed and efficiency of the Foreign Military Sales (FMS) and Direct Commercial Sales (DCS) processes would be inadequate for the expected increase in volume of AUKUS-related defense trade.

The Administration will take three steps to implement the AUKUS Trade Authorization Mechanism:

- First, identify the scope of AUKUS programs.



US NAVY PHOTO

This will optimize operations and compliance, as both government and industry will have a clear understanding of which uses/programs are authorized under this Mechanism.

- Second, identify what technologies are not eligible under this Mechanism.
- Third, identify which communities in each country would be approved for access to the technology, which includes an obligation to record what is transferred and to secure and protect the technology. This will help reduce the likelihood of unauthorized diversion of sensitive defense technologies and, if necessary, help to investigate any potential diversion.

Next, utilization of ATAM will proceed as follows:

- The exporter must check proposed transfers under AUKUS against these three basic and transparent criteria (programs, technologies, and authorized communities) that Defense and State would develop, and review with partners.
- Transfers beyond the UK or Australia, or transfer to a non-AUKUS program or a community not eligible to receive it, would require standard non-ATAM authorization.
- Based on legislation, the U.S. government would need to notify shipments under this au-

Continues on next page

Continued from previous page

thorization exceeding \$100 million at least 15 days prior to the shipment. Existing systems will be utilized to conduct congressional notification.

The AUKUS Trade Authorization Mechanism will allow DCS transfers of some items typically transferred only under FMS.

The AUKUS Trade Authorization Mechanism offers an immediate solution to expedite and secure defense transfers of U.S. defense items for AUKUS projects, leveraging existing authorities (§ 126.4 of the ITAR) “to allow seamless and speedy defense trade.”

Congressional Progress

The Senate Foreign Relations Committee has approved the transfer of nuclear-powered submarines to Australia, a move that signifies progress for the AUKUS security pact. The decision was part of the *National Defense Authorization Act*, granting Australia a unique 20-year exemption from the stringent export rules of ITAR.

Despite this progress, the *National Defense Authorization Act* is still set to encounter hurdles before receiving full Senate and House approval. Both Democratic and Republican lawmakers are locked in a fierce debate over social spending measures in the Pentagon’s defense budget, unrelated to the AUKUS agreement.

Committee Chairman Bob Menendez (D-N.J.), underscored the bill’s significance in meeting global challenges and modernizing the State Department for 21st-century demands. The proposed legislation is seen as a critical step in updating the U.S.’s diplomatic and national security capabilities, a move supported by **Ranking Member, Sen. Jim Risch** (R-Idaho).

In a strategic move to expedite approval, the AUKUS provision was included in the broader National Defense Authorization Act, rather than introduced as separate legislation. This decision is expected to speed up Congressional endorsement.

Australia’s Ambassador to the U.S., Kevin Rudd, welcomed the committee’s decision, expressing hope for the swift passage of the legislation. The transfer of submarines signifies a significant step in the implementation of the AUKUS pact, strengthening Australia’s defense capabilities in the Indo-Pacific region.

The **U.S. House Foreign Affairs Committee** approved a series of authorizations on Wednesday, July 26, aimed at accelerating the implementation of the AUKUS agreement, including the sale of up to two nuclear-powered Virginia-class submarines to Australia. This authorization was included as a provision in the broader National Defense Authorization Act, in a strategic move to speed up Congressional endorsement.

The controversial decision faced opposition from Democrats due to proposed exemptions for the U.K. and Australia from a crucial U.S. export control regime. However, Republicans in the committee advanced the legislation along party lines.

According to **Rep. Michael McCaul** (R-TX) “The nuclear sub is one thing the Chinese don’t have us beat on. We’ve got superiority with the nuclear sub. So getting that moving is hugely important for deterrence reasons.”

Despite the support, the Senate’s debate over submarine capacity complicated the passage of AUKUS authorizations. The Pentagon had previously requested Congress to attach submarine transfer authorizations to the National Defense Authorization Act for fiscal 2024.

ITAR Waivers Proposed

In addition to the submarine sale authorization, two other bills were advanced by the House Foreign Affairs Committee. These aimed to provide both the U.K. and Australia with blanket exemptions from the International Traffic in Arms Regulations (ITAR), a privilege currently only enjoyed by Canada. The committee narrowly voted to advance both bills.

The corresponding Senate bill introduced by Senate Foreign Relations Chairman Bob Menendez stops short of offering a blanket ITAR exemption, unlike its House counterparts.

“ITAR Comparable”

A June legislative proposal from the State Department, seen by Defense News, asked Congress to give Australia and Britain the ITAR exemptions only if the two countries implement their own export control regimes “that are at least comparable to those administered by the United States.”

Non-Proliferation Concerns

The International Atomic Energy Agency (IAEA) has stated it will inspect Australia's future nuclear submarines both before and after deployments, as part of a watertight agreement to ensure no fissile material is diverted for other purposes. Rafael Mariano Grossi, director general of the IAEA, stated that further negotiations are due to ensure the AUKUS deal does not conflict with non-proliferation obligations.

The Guardian reports The Aukus deal exploits a loophole in the 1968 Nuclear Non Proliferation treaty that allows nuclear fuel used for non-explosive military uses like naval propulsion to

be exempted from IAEA inspections. To limit access, nuclear fuel will be delivered to Australia in welded power units which would be installed in submarines to be assembled by Australia and ready by the 2040s.

China Objections

Meanwhile, China has voiced its strong objection to the deal, alleging that the AUKUS partners had coerced the IAEA into accepting the agreement. It remains to be seen how these geopolitical tensions will impact the final passage and implementation of the AUKUS legislation.

Visit the website links to source documents and State memo:



Committee Targets Cal-China Collaboration

Sweeping inquiry into academic operations

REP. MIKE GALLAGHER (R-WI), Chair of the Select Committee on the Chinese Communist Party, and **Rep. Virginia Foxx** (R-NC) of the Education and the Workforce Committee, recently sent a letter to the President and Chancellor of the University of California Berkeley, expressing concerns about Berkeley's joint institute with Tsinghua University and the Shenzhen government in China..

The lawmakers pointed out that the Tsinghua-Berkeley Shenzhen Institute (TBSI) provides the People's Republic of China (PRC) with easy access to Berkeley's research and expertise. They emphasized that this access potentially allows the PRC to gain economic, technological, and military advantages.

TBSI was established in 2014 to support a dual-degree program, "designed to fuel economic growth through transdisciplinary and translational research," according to the University. The program allows students to spend 2.5 years pursuing a master's degree in engineering at Berkeley and a master's of science degree at Tsinghua.

Tsinghua University was founded in 1911 with funds from the United States' Boxer Rebellion Indemnity, as a preparatory school for students the Chinese government planned to send to the United



States. The University hosts, among other programs, the prestigious Schwartzman Scholars.

Sather tower, UC Berkeley

ADOBE STOCK

Letter Details Concerns

According to the lawmakers, one of their key concerns is the resemblance between TBSI's research priorities and the PRC's science and technology goals outlined in its 13th Five-Year Plan. The alignment of these priorities raises questions about whether U.S. taxpayer dollars are inadvertently contributing to the PRC's military and technological advancements.

Continues on next page

Continued from previous page

The letter draws extensively from reporting in May by "The Daily Beast" which detailed the commercial and financial ties between Cal and Chinese entities associated with TBSI. In that piece, Robert Shaw of the Middlebury Institute questioned language about priority commercialization rights, calling it a "red flag in an export-control compliance sense."

"That sort of language sounds like the purpose of the research is IP generation versus the sharing of knowledge globally in an academic context," he said.

"Berkeley's PRC-backed collaboration with Tsinghua University raises

many red flags," reads the Congressional letter to Cal Administrators.

- "First, TBSI is engaging in research in dual-use technologies that will likely be used to advance the PRC's military or intelligence capabilities.

- Second, TBSI is collaborating with PRC universities and companies that the U.S. Government has banned from receiving sensitive U.S. technology, which raises concerns about whether TBSI may be helping such blacklisted actors to access such technologies.

- "Third, despite billing itself as an academic partnership, in practice one of TBSI's main functions is to facilitate PRC funding of Berkeley

research — all while reportedly failing to disclose funding from the city of Shenzhen and from Tsinghua.

The lawmakers expressed apprehension regarding the nature of the collaboration, stating that although TBSI is presented as a joint technology venture among educational institutions, it appears to function as a program through which the PRC pays for access to Berkeley's research and expertise.

The letter dated July 13 asks for an information trove on a timeline sure to ruin somebody's vacation schedule. **"We respectfully request that you produce documents and information sufficient to respond to the following questions no later than July 27, 2023:**

- Please produce all documents regarding contractual or investment relationships between Berkeley and TBSI, the scope of technical collaboration, procedures for licensing intellectual property in or out, non-disclosure agreements imposed by TBSI, and the management structure of TBSI. Please also provide copies of any memorandum of understanding related to TBSI, feasibility studies for TBSI, approvals for formation of TBSI, and similar documentation, as well as any annual reports, balance sheets, business licenses, social credit reports, court or administrative judgments or decisions, capital examinations, or similar documents related to the operations and activities of TBSI.

- Please provide copies of all meeting minutes for meetings among the regents of the University of California that mention TBSI.

- The Chancellor of Berkeley is listed as the co-chair of the joint management committee of TBSI.²¹ Please describe her role at TBSI and any steps she has taken to ensure compliance with U.S. export controls, including any policies, procedures, memoranda, guidance documents, or internal controls implemented or communicated to relevant personnel, researchers, and students.

- Please produce documents suf-

ficient to show all compliance and due diligence mechanisms currently in place for research taking place at TBSI in the U.S. and in the PRC.

- If compliance and due diligence mechanisms are currently in place, when were they implemented and by whom?

- Was the University of California (UC) aware of Berkeley's collaboration with PRC universities on the Entity List? Did UC approve of this collaboration?

- Was UC aware of the presence of representatives from companies on the Entity List on TBSI's Industrial Advisory Board? Did UC or UC Berkeley approve the board membership? A TBSI team won a contest in April 2023 for 7 nanometer chip technology. Does Berkeley consider this activity to be in violation of the October 7th, 2022, restrictions on advanced chip manufacturing and research?

- A 2018 Defense and Counterintelligence Security Agency document states that Tsinghua University has previously sought sensitive, dual-use, or export-controlled materials and components. Has TBSI engaged in any research that could be, or has been, used by the PRC for military applications?

- Has TBSI fundamental research in the U.S. or elsewhere involved the use of export-controlled technologies or

software?

- Is TBSI conducting applied research in the PRC that would be covered by U.S. export control laws if this research were conducted in the United States?

- Has any TBSI research generated technology or goods subject to export controls? Please describe the process by which TBSI determines which research projects to undertake and which research areas to prioritize.

- Please produce all records maintained regarding TBSI alumni and their current or past affiliations.

- TBSI's Industrial Advisory Board features companies currently or formerly on the Commerce Department Entity List such as PRC telecom firms Huawei and ZTE. Please describe the role these companies play in TBSI's operations and/or research.

- Has any of TBSI's research been sponsored by entities on the U.S. Entity List? If so, please provide a description of the sponsoring company and project.

- Has any of TBSI's research been sponsored by PRC entities that are engaged in human rights abuses, such as Tencent?

- How does Berkeley manage its interests in intellectual property co-developed with TBSI? Has TBSI licensed any intellectual property (patents, trade secrets, semiconductor layout designs, etc.)? Please describe,

including by providing any Chinese or foreign patent numbers, any intellectual property that has been licensed, the terms of the license agreement and to whom the intellectual property has been licensed.

- Please provide a list of any patents or patent applications made in China using technology provided by or developed cooperatively with TSBI that were filed anonymously in the Chinese patent office.

- Has any PRC entity appropriated or attempted to appropriate intellectual property generated by Berkeley researchers for any reason? Please provide a detailed list of these intellectual property items, including any patent applications first filed in China for which the Chinese government denied approval for a foreign filing in the U.S. or elsewhere, whether or not any such intellectual property was misappropriated in China.

- Please identify any Berkeley employees, contractors, or researchers involved with TBSI who have U.S. security clearances, or are subject to U.S. deemed export licenses, or otherwise have access to information which the U.S. protects from disclosure to foreign nationals or interests. When applying for research funding from federal grant

providing agencies, have Berkeley faculty members who work as core principal investigators (PIs) disclosed their involvement in TBSI and any financial compensation they received as consultants?

- Please provide all proposals for federal funding awarded to Berkeley faculty members while working in any capacity for TBSI.

- Please provide all contracts or agreements for Berkeley faculty members who have worked or are working as Core PIs, consultants, or in any other capacity at or for TBSI, including how much each has been paid.

- Please list all organizations or individuals that provided funding for the salary of Berkeley Core PIs involved with TBSI.

- Please advise if TBSI researchers have been subjected to any blocking orders from the PRC government to require them to perform tasks that are contrary to U.S. export control laws, such as providing assistance to North Korea, Russia, or Iran. Please describe any procedures in place for TBSI PIs to handle such potential conflicts.

- Provide a list of any scientific publications in Chinese and English that were authored or co-authored by Berkeley researchers in collaboration

with TBSI. Please note in this list any research that is published only in China and is not available outside of China due to restrictions imposed by China National Knowledge Infrastructure or other government authority.

- Please provide a list of all foreign funding that Berkeley has received for TBSI since its inception, including the date received, amount, and source.

- Please describe the process by which the University of California assesses whether to report TBSI funding or contracts under Section 117 of the Higher Education Act.

- How much has Tsinghua Education Foundation North America (TEFNA) raised for TBSI from 2014 to date?

- Has the University of California disclosed TEFNA's contributions to the Department of Education under Section 117? If not, why not?

- Please list the specific research agreements that TEFNA has sponsored.

- Please provide a translation of the Chinese language website of TBSI (<https://www.tbsi.edu.cn>) and explain the differences between that website and the English content, particularly regarding the technologies being researched and the role of Berkeley in the operation of TBSI.

BRIEF

Europe Adopts Data Privacy Deal

► The European Commission has adopted its adequacy decision for the European Union-US Data Privacy Framework, concluding that the U.S. ensures an adequate level of protection — comparable to that of the European Union — for personal data transferred from the EU to U.S. companies under the new framework.

“On the basis of the new adequacy decision, personal data can flow safely from the EU to U.S. companies participating in the Framework, without having to put in place additional data protection safeguards,” the commission said.

The EU's announcement comes following the U.S. government's affirmation that it has fulfilled its commitments under the framework.

President Biden praised the EU's announcement, saying it “represents the culmination of years of close cooperation between the United States and the European Union, and affirms the strength of our transatlantic relationship founded

on our shared democratic values and vision for the world.”

U.S. companies will be able to join the EU-U.S. Data Privacy Framework by committing to comply with a detailed set of privacy obligations, for instance the requirement to delete personal data when it is no longer necessary for the purpose for which it was collected, and to ensure continuity of protection when personal data is shared with third parties.

EU individuals will benefit from several redress avenues in case their data is wrongly handled by U.S. companies. This includes free-of-charge independent dispute resolution mechanisms and an arbitration panel.

In addition, the U.S. legal framework provides for a number of safeguards regarding the access to data transferred under the framework by U.S. public authorities, in particular for criminal law enforcement and national security purposes. Access to data is limited to what is necessary and proportionate to protect national security.

Treasury Releases CFIUS Annual Report for 2022

THE DEPARTMENT OF THE Treasury, as Chair of the Committee on Foreign Investment in the United States (CFIUS), released its Annual Report to Congress for calendar year 2022.

The Annual Report highlights key indicators of the CFIUS process and provides statistics on transactions that were filed with the Committee in 2022.

The Committee's workload remained high with a record number of filed transactions based on the expanded jurisdiction provided by the Foreign Investment Risk Review Modernization Act (FIRRMA), mandatory filings in certain instances, and more sophisticated processes for identifying non-notified transactions.

"In 2022, the Committee continued to review record numbers of filings. We sharpened due diligence on investors, tackled sophisticated technologies and national security risks, and launched a number of reviews to assess potential non-compliance with CFIUS regulations," said **Assistant Secretary for Investment Security Paul Rosen**.

Key highlights from 2022 include the following:

CFIUS reviewed a record number of covered transactions with a total of 440 notices and declarations of covered transactions or covered real estate transactions. Parties filed using the short-form declaration process in 154 instances and filed through a notice in 286 instances. The short-form process saw a seven fold increase from the 20 declarations the committee received in 2018.

The Finance, Information, and Services sector accounted for 52 percent or 149 of the 285 non-real estate CFIUS notices. Within this sector, Professional, Scientific, and Technical Services continued to be the largest subsector, accounting for 44



percent or 66 notices.

The other top subsectors in 2022 were Telecommunications at 15 percent or 22 notices, followed by Publishing Industries (except Internet) at 13 percent or 20 notices. All other subsectors fell below 10 percent of notices.

Manufacturing sector accounted for 29 percent or 84 of the 285 non-real estate CFIUS notices. Within Manufacturing, the subsector with the most notices remained Computer and Electronic Product Manufacturing, accounting for 37 percent (31 notices). The next highest subsector was Transportation Equipment Manufacturing, accounting for 17 percent (14 notices).

The Mining, Utilities, and Construction sector accounted for 13 percent

or 36 of the 285 non-real estate CFIUS notices. Within this sector, the Utilities subsector accounted for 67 percent of the sector (24 notices). The Support Activities for Agriculture and Forestry subsector, Oil and Gas Extraction subsector, and Specialty Trade Contractors subsector were the next highest subsectors with 8 percent or three notices each in 2022.

In 2022, the highest number of Covered Transaction notices were from Singaporean investors, accounting for 12.9 percent (37 notices), followed by Chinese and British investors, accounting for 12.6 percent and 6.3 percent, respectively (36 and 18 notices). For the three-year period from 2020 through 2022, the highest number of notices were from Chinese investors, accounting for 13.0 percent (97 notices), followed by Japanese and Singaporean investors, accounting for 8.1 percent each (60 notices each).

Notices from China, Japan, and Singapore together accounted for approximately 29 percent of notices filed from 2020 to 2022. The distribution of notices from these

countries were generally consistent with the overall distribution of notices across the four industry sectors although Canada had the most notices in the Mining, Utilities and Construction sector, consistent with previous years' reports.

The Committee enhanced its focus on non-notified transactions to detect and assess national security risks posed by foreign investment. These matters often required mitigation or other measures to resolve national security risks. One notice was rejected by CFIUS in 2022.

While there were no presidential actions taken on transactions, a number of transactions were voluntarily abandoned or divested based on CFIUS's national security determinations.

2022 developments that go beyond the data in the Report include:

In January 2022, the Committee identified New Zealand as an "excepted foreign state" and determined that Australia and Canada are and will remain excepted foreign states absent further Committee action and notice in the Federal Register;

In June 2022, Treasury hosted the inaugural CFIUS conference, which provided the Committee an

opportunity to engage with approximately 500 stakeholders on CFIUS process, risk analyses, and other topics;

In September 2022, President Biden issued an executive order highlighting several national security risk factors that the Committee shall appropriately consider when reviewing transactions; E.O. 14083, "Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States."

While this Executive Order did not change CFIUS authorities, it sharpened the Committee's focus on two national security factors already codified in Section 721(f) (supply chain security and resiliency and U.S. technological leadership) and highlighted three additional national security factors (aggregate industry investment trends, cybersecurity, and sensitive data)

In October 2022, Treasury released its first ever enforcement and penalty guidelines, which provide the public with information on how the Committee assesses violations of the laws and regulations that govern transaction parties, including potential breaches of CFIUS mitigation agreements.

CFIUS

Bill to Expand to Land Purchases

REPRESENTATIVE MIKE GALLAGHER (R-WI), Chairman of the Select Committee on the CCP, and **Representative Mike Thompson** (D-CA) unveiled a key piece of legislation that aims to broaden the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS).

The new law, known as the Protecting U.S. Farmland and Sensitive Sites From Foreign Adversaries Act, comes as a response to growing concerns over foreign adversary entities acquiring land near sensitive sites, including military facilities.

The proposed bill represents the first amendment to the CFIUS mandate since 2018 and includes a cross-party group of co-sponsors, from both rural and urban districts.

"The United States cannot allow foreign adversaries like the Chinese Communist Party and its proxies to acquire real estate near sensitive sites like military bases or telecom infrastructure,

potentially exploiting our critical technology and endangering our servicemembers," said Rep. Gallagher.

"This bill gives CFIUS jurisdiction over foreign adversary real estate transactions to guard against the threat of the CCP and other adversaries purchasing land for malign purposes, **and it also encourages CFIUS to consider food security issues as it evaluates the national security risk of a given transaction.**"

The proposed legislation includes the following provisions:

- It expands CFIUS' authority to oversee all land purchases by foreign adversary entities, barring exceptions for urban real estate and single housing units.
- It authorizes CFIUS to consider U.S. food security, including through biotechnology acquisitions, as a factor in its national security

Continues on next page

Continued from previous page

reviews. It also necessitates the Secretary of Agriculture's vote in CFIUS reviews of transactions involving farmland or agriculture technology.

- It sets a “presumption of non-resolvability” for CFIUS reviews, which means a higher approval threshold for transactions by a foreign adversary entity purchasing land near sensitive sites.

- It mandates CFIUS filing for foreign adversary entities making land purchases near sensitive sites to keep CFIUS informed about ongoing real estate purchases.

- It expands the list of sensitive national security sites designated for CFIUS jurisdiction.

The term “foreign adversary” is defined as:

The People’s Republic of China, including all Special Administrative Regions Cuba; Iran; North Korea; The Russian Federation; and Venezuela during any period in which Nicolás Maduro is President of the Republic.

The term “foreign adversary entity” is described as:

- A foreign adversary;
- A foreign person subject to the jurisdiction of, or organized under the laws of, a foreign adversary; and
- A foreign person owned, directed, or con-

trolled by an entity described in the previous two points.

The expanded definition of a “sensitive site” includes:

- Military installations; Special use airspace; U.S. intelligence facilities
- Research and development centers
- Airports; Maritime ports
- Significant telecommunication facilities; Electric power plants
- *Any other sites as determined by the Secretary of Defense or the Secretary of Homeland Security.*

Sponsors include: Rep. Dan Newhouse (R-WA), Rep. John Garamendi (D-CA), Rep. Dusty Johnson (R-SD), Rep. Ed Case (D-HI), House GOP Conference Chair Elise Stefanik (R-NY), Rep. Jim Costa (D-CA), Rep. Frank Lucas (R-OK), Rep. Jimmy Panetta (D-CA), Rep. Rob Wittman (R-VA), Rep. Jason Crow (D-CO), Rep. Randy Feenstra (R-IA), Rep. Salud Carbajal (D-CA), Rep. Jim Banks (R-IN), Rep. Salud Carbajal (D-CA), Rep. Mary Pelto (D-AK), and Rep. Ashley Hinson (R-IA).

Missing from the list of supporters was **Rep. Beth Van Duyne** (R-TX) who recently introduced the Protecting American Farmland Act proposing a 60% excise tax on “Countries of Concern” attempting to buy American farm and ranch land.

Visit the website for links to source documents and full text of the bill:



Visit the website for the whole story, links to source documents and text of the bill:



BRIEFS

Bipartisan FDI Promotion Advanced

► **U.S. Senators Todd Young (R-Ind.) and Gary Peters (D-Mich.)** have introduced the *Global Investment in American Jobs Act of 2023*, a bipartisan bill with the objective of boosting America's global competitiveness and attracting foreign direct investment to the nation.

The legislation aims to strengthen the U.S. economy by encouraging international companies to invest in the country, thereby creating more jobs, advancing domestic research and development, and promoting exports of American-made goods.

The bill calls for a comprehensive government-wide review of strategies to enhance America's attractiveness to foreign investors. The Secretary of Commerce will be tasked with conducting this review and subsequently reporting the findings to Congress.

The key provisions of the bill include

- identifying and removing unnecessary barriers to foreign direct investment from responsible private sector entities based in trusted countries.

- Additionally, the legislation aims to promote policies that will maintain the United States' status as a premier global investment destination,

- strengthen the nation's leadership in advanced technologies like artificial intelligence and quantum computing,
- reduce dependency on supply chains from foreign adversaries like China, and
- encourage an open investment policy with private-sector entities based in trusted countries.

The Global Investment in American Jobs Act has garnered bipartisan support, with U.S. Representative Greg Pence (R-IN-06) introducing a companion legislation in the House of Representatives. The House recently passed the bill with an overwhelming vote of 386-22.

Organizations including Autos Drive America, Global Business Alliance, Information Technology Industry Council, National Association of Manufacturers, and the U.S. Chamber of Commerce, have expressed support for the legislation.

BRIEFS

EXPORT-IMPORT BANK

EXIM Backstops Swiss Commodity Trader \$400 million

► The Board of Directors of the Export-Import Bank of the United States announced their approval of a \$400 million dollar credit guarantee for the trading book of a Swiss commodity trader.

Financial Institution Buyer Credit (FIBC) policies backstop credit lines for Geneva-based **Trafigura** to broker natural gas purchases from the U.S. “primarily to European Buyers,” according to the EXIM announcement.

The subsidies to Trafigura’s bankers, Citibank and Credit Agricole “could support over 12,000 U.S. jobs,” according to EXIM. Each policy is for \$200 million, with a 90 percent guarantee, for a taxpayer exposure of \$360 million.

Trafigura, which reported profits of \$7 billion last year, has been under investigation by the U.S. Department of Justice for commodity price manipulation, and was one of the biggest buyers of Russian oil before the war. The firm continues to trade with Moscow, according to reporting by the *Financial Times*, most recently importing Russian diesel to Argentina.

The EXIM board also approved a loan commitment of more than \$238 million to support the export of Boeing B737 MAX 8 aircraft to **SunExpress Airline** in Turkey. According to EXIM, this transaction could support around 1,100 American jobs nationwide.

Bank Loosens Repayment Terms

► The US Export-Import Bank will begin offering **longer repayment terms and additional flexibilities** for most transactions.

The new flexible financing terms and conditions are a result of a modernized agreement with Organization for Economic Cooperation and Development Arrangement Participants.

Under the updated agreement, ExIm will be able to offer maximum repayment terms up to 22 years (up from the previous maximum of 18 years) to an expanded set of technologies offering the greatest climate change mitigation benefit.

Many nuclear energy projects will also be eligible for up to 22-year maximum repayment terms. While necessary for project viability, loans and guarantees of this duration are not always available from private lenders in the commercial market.

The updated climate change mitigation project classes now include projects related to energy storage, grid efficiency, battery production and recycling, clean hydrogen and ammonia production and



storage, low emission manufacturing, zero and low emission transport and clean energy minerals and ores.

The agreement also provides more flexible financing terms — up to 15 years for most types of transactions, up from a previous maximum of 10 years — as well as longer grace periods and larger balloon payments, and it will reduce the minimum premium rates for higher credit risk borrowers using longer repayment terms.

Nuclear energy projects will be eligible for up to 22-year repayment terms.

ADOBE STOCK

Bank head Tours Angola

► EXIM President and Chair Reta Jo Lewis traveled to Luanda, Angola, where she met with government leaders, private sector companies and external stakeholders to highlight EXIM’s activity in the region. She also spoke at the Luanda International Trade Fair.

In June, Exim approved a direct loan for more than \$900 million to the Ministry of Energy and Water of the Republic of Angola to support the construction of two photovoltaic solar energy power plants. The project will generate over 500 megawatts of renewable power.

The project — initially announced during the 2022 G7 Summit by the Government of Angola, New Orleans consultants **AfricaGlobal Schaffer**, and Miami based solar developer **Sun Africa** — supports EXIM’s China and Transformational Exports Program (CTEP), a congressionally mandated program to support U.S. exporters facing foreign competition from China.

Sun Africa recently signed an EPC contract with the Government of Nigeria for 5 gigawatts of solar generation and 2.5 gigawatts of battery storage. U.S. EXIM Bank approved a \$1.5 billion loan to finance that development with the Ministry of Industry, Trade, and Investment of Nigeria.

Raimondo: No Timetable for Added China Controls

China Hawks squawk, call for curbs

Visit the website for links to source documents and text of the letter:



Commerce Secretary Gina Raimondo

THE ADMINISTRATION is not operating on a timetable for releasing highly-anticipated new export control rules on cutting-edge technology, **Commerce Secretary Gina Raimondo** said in July at a program sponsored by the American Enterprise Institute.

The focus instead is on getting the final rules right, so that U.S. national security is protected but companies are not prevented from selling readily-available technology.

Commerce is engaging closely with industry and stakeholders as it crafts the final rules. “What we want to do is be incredibly targeted,” Ms. Raimondo said. “We don’t want to control anything you don’t have to control, but we don’t want to let anything through the gates that we want to control.”

Artificial intelligence is “is a huge part of this,” she added. “We’re the global leader in AI and we want to stay that way.”

Ms. Raimondo stressed that U.S. export controls on cutting edge technology is “not about

holding China back,” as Chinese officials claim. But Beijing is carrying out a military-civil fusion strategy that depends on access to the most sophisticated U.S. technology for military use. “We are not going to allow that,” she stated.

She also warned that China’s aggressive use of industrial subsidies will create a glut of semiconductor chips. “The amount of money that China is pouring into subsidizing what will be an excess capacity of mature chips and legacy chips, that’s a problem that we need to be thinking about and working with our allies to get ahead of,” she said.

China Hawks Call for Action

Friday **Rep. Mike Gallagher** (R-WI) and **Rep. Raja Krishnamoorthi** (D-IL), Chair and Ranking Member of the Select Committee on the Chinese Communist Party, sent a letter to Secretary Raimondo urging the Administration to tighten export controls first announced on Oct. 7, 2022 that restricted advanced semiconductors and equipment from being exported to the People’s Republic of China (PRC).

The lawmakers cite concern that PRC technology firms have identified workarounds to evade the export control rules, allowing the country continued legal access to advanced semiconductors that can efficiently train artificial intelligence models.

The lawmakers requested:

- In tandem with consideration of other relevant parameters, the advanced computer rule threshold for the bidirectional transfer rate of 600 Gbyte/s to be lowered sufficiently to prevent clever engineering that bypasses the regulations set on October 7.

- The Administration consider measures to ensure cloud computing services are not used by Chinese firms to simply outsource their advanced computing needs.



BIS GUIDANCE

Best Practices for License Applications for Medical-Related Items

BIS HAS PUBLISHED best practices for submitting export license applications for medical-related items destined for Russia, Belarus, and the occupied/covered regions of Ukraine.

It reflects the U.S. Government's position that the Russian and Belarusian people are not the target of export controls imposed on Russia and Belarus due to their activities in Ukraine.

Key takeaways are:

End-Use/User Statements: Exporters must certify they have carried out due diligence to ensure the medical facilities listed as ultimate consignees or end-users are civilian facilities providing direct patient care.

License Scope: It is generally advised to limit licenses to a one-year validity period due to the potential risk of diversion in a dynamic wartime environment. Applications with a relatively narrow transaction scope can be evaluated faster by the reviewing agencies.

Export Item Grouping: When listing varying categories of items, it's recommended to group them into like categories for easier evaluation by reviewing agencies. Clear and specific item descriptions, including the use of Harmonized System (HS) codes, can expedite the review process.

Direct Patient Care: Applications that clearly demonstrate the end users will use the items to provide direct patient care to civilian patients in a civilian treatment facility are processed more efficiently.

HS Codes: The use of correct HS codes in license applications is important to avoid potential misclassification of items.

Best Practices Checklist: The document provides a checklist for exporters to follow when preparing their license applications, with considerations such as whether the exporter has provided a statement certifying the medical facilities on the application are civilian facilities providing direct patient care, and whether they have provided an accurate description of how the items would be used for direct patient care.



ADOBE STOCK

Best Practices Checklist

- Have you provided a statement certifying that the medical facilities on the application are civilian facilities providing direct patient care only to civilian patients?
- Are the item quantities scoped to what would be used over the period of 1 year?
- Do the items for export have an identifying description in the Technical Description Block?
- Did you scope the license to minimize the risk of diversion to unauthorized end users/end uses?
- For items controlled by HS code, have you included the HS code that covers your items and the section of the EAR where that HS code is referenced?
- Did you provide a description of how the items would be used for direct patient care?
- Have you explained the role of any parties that do not provide direct patient care?

This guidance is intended to help draft applications that can be reviewed efficiently, but does not impose or create additional requirements for license applications.

All applications received by BIS will be reviewed consistent with the provisions of Executive Order 12981 and the relevant provisions of the EAR.

Visit the website for links to source documents and the BIS document:



Export Controls — Myth & Fact

State Department Primer Released

WITH EVERYONE IN WASHINGTON now holding an opinion on Export Controls, the **State Department's Bureau of Political-Military Affairs** published a useful one pager of talking points on export controls, including the following items:

Under the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR), defense export controls are a key tool to safeguard technologies that provide a critical military or intelligence advantage to the U.S.

MYTHS AND FACTS

MYTH: Obtaining an export license for Direct Commercial Sales (DCS) from the Department of State takes too long under the ITAR.

FACT: There are many exemptions available under the ITAR to enable speedy and secure defense trade, including the exemption at ITAR section 126.4 which supports exports by or for the U.S. Government.

• For DCS defense trade, or defense trade subject to the ITAR, there are 50+ ITAR exemptions and other authorization mechanisms available for some of our closest allies that don't require a license from the Directorate of Defense Trade Controls (DDTC).

For example, there is an exemption specifically designed to facilitate license-free transfers for both classified and unclassified defense articles for programs like AUKUS (under ITAR 126.4).

Another example is the Open General License (OGL) Pilot Program. Recently extended by three years, OGLs enable certain qualifying re-exports and re-transfers to occur without requiring specific authorization from the Department of State.

MYTH: Military exercises must build in a buffer of anywhere between 6 to 18 months to obtain the necessary U.S. export control approvals prior to the commencement of the exercise.

FACT: The Department of State published a proposed rule (Public Notice 11801 (87 FR 77046), December 16, 2022) that, if implemented as a final rule, would state that taking a defense article on deployment or exercises, assuming certain conditions are met, is

not a re-export or re-transfer subject to the ITAR.

MYTH: The ITAR unnecessarily prevents U.S. companies from building munitions production facilities abroad.

FACT: The ITAR provides an authorization mechanism for the Government of the United States to authorize the manufacture of U.S.-origin defense articles, including munitions abroad.

However, before such an authorization can be provided, the U.S. manufacturer and a foreign party need to sign a contract for such activities.

The Department of State does not review or authorize hypothetical business arrangements that have not been finalized or agreed to by the parties. Coproduction facilities are often offset arrangements to FMS cases and require licenses.

MYTH: Due to ITAR restrictions, foreign companies and government entities who receive U.S.-origin defense technology are unable to allow skilled dual nationals to work on projects that require access to such technology.

FACT: There is a specific ITAR exemption that enables dual nationals to work on projects with U.S.-origin defense technology.

In addition, there are additional licenses and authorizations available from DDTC for dual and third-country national employees if they don't want to use the exemption.

MYTH: The ITAR controls non-sensitive items such as bolts and screws, which hinders production, maintenance, and refurbishment timelines.

FACT: Over the last decade, the executive branch conducted a complete review of the commodities and activities

described on the United States Munitions List (USML) and controlled under the ITAR.

• Commodities and activities found to not provide a critical military or intelligence advantage were moved to the Commerce Control List administered by the Department of Commerce and are no longer subject to the ITAR's jurisdiction.

• As a result of this review, the Department of State went from processing over 85,000 licenses to around 20,000 a year, dramatically reducing the licensing burden on industry.

MYTH: Export controls are not necessary to transfer sensitive technology to close partners and allies since our countries have similar foreign policy and national security objectives.

FACT: The application of export controls to our most sensitive technologies does not demonstrate a lack of trust in our partners and allies. Rather, it reflects our awareness that malign actors are intent on acquiring sensitive technology that we, along with our partners and allies, develop.

The threat of proliferation and misuse of critical technologies by malign actors is a serious concern for all. For example, an AI algorithm capable of creating drone swarms would cause great harm in the wrong hands.

Visit the website for the full story and links to source documents:



FOCUS ON SANCTIONS

SANCTIONS COMPLIANCE

Note Issued on Voluntary Self-Disclosure Policies

JUSTICE, COMMERCE AND THE TREASURY Department issued a joint compliance note focusing on the voluntary self-disclosure policies that apply to US sanctions, export controls and other national security laws, including recent updates to some of those policies.

The July 26 note marks the second collective effort by the three agencies to inform the private sector about enforcement trends and provide guidance to the business community on compliance with US sanctions and export laws.

The compliance note describes the voluntary self-disclosure policies of Commerce's Bureau of Industry and Security, the Justice Department's National Security Division and Treasury's Office of Foreign Assets Control, and highlights recent updates related to these policies.

It also highlights the **Financial Crime Enforcement Network's Anti-Money Laundering and Sanctions Whistleblower Program**, which incentivizes individuals in the United States and abroad to provide information to the government about violations of US trade and economic sanctions, in addition to violations of the Bank Secrecy Act.

The note underscores the importance of an effective and robust compliance program, the agencies said. If a company discovers a potential violation, whether it is an administrative or criminal violation, that company must promptly disclose and remediate. Not only does such reporting make the disclosing company potentially eligible for significant mitigation, but it also alerts national security agencies to activities that may pose a threat to the national security and foreign policy objectives of the US government.

"American businesses play a vital role in defending our national security, because they are gatekeepers for sensitive technologies and key participants in the financial system," said Assistant Attorney General for National Security Matthew Olsen. "Responsible companies that come forward as soon as they learn of potential sanctions and export control violations will benefit from the protections of these self-disclosure policies."

Tri-Seal Compliance Note: Voluntary Self-Disclosure of Potential Violations.



OFAC Heavies Up Russia Sanctions

TREASURY'S OFFICE OF FOREIGN Asset Control designated dozens of entities as Washington continues to apply economic pressure on Moscow for its invasion of Ukraine. The July 20 actions follow a May 19, 2023 Supplemental Alert, where Treasury's Financial Crimes Enforcement Network (FinCEN) and the U.S. Department of Commerce's Bureau of Industry and Security (BIS) identified certain high

priority items, primarily based on the Harmonized System (HS) code classification of components from Russian weapons systems recovered on the battlefield in Ukraine, to assist financial institutions in identifying suspicious transactions relating to possible export control evasion.

Items described by these HS codes have been found in multiple Russian weapons systems used against

Ukraine. Many of the entities designated have transferred certain of these high priority items to Russia-based end-users.

Russia's Use of Kyrgyz Republic-based Entities to Acquire Dual-Use Technology

Three entities based in the Kyrgyz Republic have been frequent
Continues on next page

Continued from previous page

exporters of controlled electronics components and other technology to Russia. Some of these shipments have subsequently supplied sensitive dual-use goods to entities in Russia's defense sector.

Additional Sanctions Evasion Facilitators include:

- A UAE-based engineering and services company and AK Microtech (AKM) a Russia-based firm that specializes in transferring foreign semiconductor technology to Russian microelectronics production companies. AKM uses non-Russian intermediaries to obfuscate Russian recipients.

Russia-Based Importers of Dual-Use Items

OFAC continues to target Russia-based entities that import dual-use technology from abroad. Eleven Russia-based entities were designated in this action.

Munitions Factories and Defense Technology Sector

Russia-based entities designated for operating in the defense and related materiel sector include four producers of explosives and ammunition, a producer of components for rocket systems, missiles, and bombs. And the **National Centre of Laser Systems and Complexes (Astrofizika)** a research and development center focused on laser and optical technologies.

OFAC is also targeting entities in key industries such as aerospace, quantum technologies, and advanced computing including research institutes and other entities that support Russia's research and development of high-technology goods. Designations include **six government institutes focused on physics and informatics** and a private company involved in superconducting nanotechnology

Financial Institutions

Five Russian banks were designat-

ed, including Tinkoff Bank, partially owned by U.S.-designated Vladimir Olegovich Potanin.

Metals and Mining Sector

Ural Mining and Metallurgical Company one of Russia's top producers of metals such as copper, zinc, gold, and silver, and affiliates involved in the non-ferrous metals processing industry, as well as a Russia-based UMMC subsidiary involved in the refining of precious metals, cathodes, and billion products.

Equipment and Chemicals for the Energy Industry

Seven Russia-based manufacturers of energy industry equipment were designated, as well as four manufacturers of energy-related refining agents and **Tyumen Petroleum Research Center**, Rosneft's corporate research and design institute. TPRC, which is involved in technology development, performs field engineering and support for geological survey processes and is involved in the development of oil and gas fields in Russia and elsewhere for Rosneft subsidiaries.

Targeting a Facilitator of Investment in Russia's Extractive Industries

The **Fund for Development of Energy Complex Energy (Fund Energy)** is a Russia-based investment house that invests in energy, oil and gas, and mining enterprises and infrastructure facilities.

For source information and links to individuals and entities sanctioned or property identified, scan the code or go to: exportprac.com/stories/ofac-heavy-up-russia-sanctions.10800



PHOTO: GORAN SRDANOV

Lead munitions for rifles

ENFORCEMENT

OFAC

New Video Series: 'Introduction to OFAC'

OFAC HAS RELEASED the first episode of its "Introduction to OFAC" web series, a series of short videos created to provide viewers with a high-level introduction on the fundamentals of OFAC and sanctions implementation.

This episode, available here, introduces viewers to OFAC and its place within the U.S. government, as well as its history, mission, and relationship with the public.



U.S. DEPARTMENT OF THE TREASURY

Images are from the video "Introduction to OFAC" series Episode 1: The Office of Foreign Assets Control hosted by OFAC Director Andrea Gacki.

Scan the code for more



information on this series from OFAC Director Andrea Gacki and Deputy Director

Bradley Smith and to see the video, or please go to: www.exportprac.com/stories/ofacs-new-video-series-introduction-to-ofac,10834



OFAC Chief Moves to FinCEN

THE U.S. TREASURY Department announced that **Andrea Gacki** has been appointed as the new Director of the Financial Crimes Enforcement Network (FinCEN).

Previously, Gacki served as the head of the Office of Foreign Asset Control (OFAC),



an arm of the Treasury Department responsible for implementing and enforcing economic sanctions. She succeeds **Himamauli "Him" Das**, who has been serving as acting director for the last two years.

FinCEN, the U.S.'s primary financial intelligence unit and

anti-money laundering standard setter, has grappled with increased demands and regulatory responsibilities in recent years. The appointment of Gacki, a widely respected leader with extensive experience in the field, is seen as a significant boost for the bureau.

In her new role, Gacki faces the **Continues on next page**

Continued from previous page significant task of implementing the bipartisan Corporate Transparency Act. This legislation aims to counteract the use of anonymous shell entities in illicit activities by requiring such entities to disclose their true, or "beneficial," owners to a secure directory at FinCEN. The Treasury Department has set a January deadline for the launch of this directory.

Additionally, FinCEN is responsible for ensuring compliance with anti-money laundering legislation across the vast U.S. real estate and

private investment markets, a commitment outlined in the 2021 U.S. Strategy on Countering Corruption.

Gacki's appointment has been hailed by financial transparency and anti-corruption advocates. **Ian Gary**, executive director of the FACT Coalition, described the appointment as a "crucial step to empower FinCEN to better safeguard the U.S. financial system." He expressed confidence in Gacki's ability to continue the momentum and deliver the necessary reforms to root out illicit money from the U.S. markets.

Zoë Reiter, co-founder of the Anti-Corruption Data Collective, said she looks forward to Gacki taking on this critical role and urged her to prioritize addressing the opacity of the private investment sector, a significant challenge in safeguarding national security.

Gacki's appointment marks the end of a period of uncertainty in FinCEN's leadership. The transition is expected to further empower the agency to fulfill its mission of combating financial crimes and illicit activities in the U.S. financial sector.

Defense Contractors Settle Anti-Boycott Charges



See the Order, Settlement Agreement and Proposed Charging Letter for Profense here:



PROFENSE **THE BUREAU OF INDUSTRY AND SECURITY (BIS)**, declared the enforcement of financial penalties against two defense companies, resolving alleged infractions of the antiboycott regulations of the Export Administration Regulations (EAR). The violations reportedly took place at a 2019 trade show in Bahrain.

Profense LLC, a Phoenix-based gatling-style machine gun manufacturer, has agreed to pay a civil penalty of \$48,500, settling four allegations of breaching antiboycott regulations. B.E. Meyers & Co, Inc., a photonics defense contractor in Redmond, WA, will pay \$44,750, settling three al-

legations. Both settlements are detailed in BIS's Proposed Charging Letters.

Both Profense and Meyers voluntarily reported the actions to BIS, collaborated with the investigation by the BIS Office of Antiboycott Compliance, and took remedial measures after identifying the problematic conduct. These proactive steps significantly reduced the penalties.

Assistant Secretary for Export Enforcement, Matthew S. Axelrod, expressed, "Today's penalties send a clear message to those receiving boycott requests, even as a participant in a trade show: You must not furnish prohibited information and you must report any such requests to BIS."

According to the settlements, both companies admitted to the allegations outlined in the Proposed Charging Letters, which included the provision of information about their business relationships with boycotted countries or blacklisted individuals, and their failure to report requests to support a foreign boycott of a country friendly to the United States.

Specifically, while participating in a 2019 Bahrain trade show, both companies certified to their freight forwarder that the goods for display were not of Israeli origin nor manufactured by a company on the "Israeli Boycott Blacklist," which is prohibited by Section 760.2(d) of the EAR. They also failed to report the receipt of such a request as required by Section 760.5 of the EAR

BRIEFS

Deutsche Bank Fined for AML Violations

► The Federal Reserve Board has announced two enforcement actions against **Deutsche Bank AG**, its New York branch, and other U.S. affiliates.

The Board issued a consent order and a \$186 million fine based on unsafe and unsound practices and violations of the Board's 2015 and 2017 consent orders with Deutsche Bank relating to sanctions compliance and anti-money laundering controls.

The Board found that Deutsche Bank made insufficient remedial progress under the 2015 and 2017 consent orders and had deficient anti-money laundering internal controls and governance processes relating to its prior relationship with the Estonian branch of Danske Bank. Separately, the Board announced a Written Agreement to address other general deficiencies relating to Deutsche Bank's governance, risk management, and controls.

Training Mandated for Unlicensed Export to S. Korea

► A Washington State man received suspended punishment for export violations. **Jaeyoun Jung**, of Puyallup faces a two-year denial of his export privileges, suspended for a two-year probationary period, then waived, provided that Jung has not committed another violation, and has completed an export controls compliance training.

On one occasion on or about Oct. 3, 2018, Jung exported from the U.S. to South Korea optical magnifiers without the required BIS license.

At all times pertinent to the transaction at issue, these items were subject to the Regulations, classified on the Commerce Control List (the "CCL") under Export Control Classification Number ("ECCN") 0A987.e, and controlled for Crime Control ("CC") reasons. The items were valued in total at approximately \$10,947. A BIS license was required to export the items to South Korea.

OFAC Sanctions Balkan Businessman

► Treasury's Office of Foreign Assets Control (OFAC) designated **Jordan "Orce" Kamcev**, in North Macedonia, pursuant to Executive Order (E.O.) 14033. Mr. Kamcev has been cited by Forbes as the "Richest Person in North Macedonia," with interests in media, banking, energy, water and real estate.

According to OFAC, Kamcev has engaged extensively in corruption, including abuse of office, money laundering, and other offenses for more than a decade starting in the early 2000s.

In 2022, Kamcev was convicted in the "Vodno Land

Parcels" trial for participating in a money laundering scheme linked to an illicit purchase of land. Kamcev also pleaded guilty to aggravated abuse of office in the "Empire Case," in which he was suspected of criminal association, fraud, money laundering, and other crimes related to his businesses.

Additionally, Kamcev used his corruptive influence and wealth to manipulate North Macedonia's judicial system in his favor. In 2020, the head prosecutor of the Special Prosecutor's Office (SPO) was charged for accepting a bribe from Kamcev and testified that Kamcev paid money in exchange for favorable arrest conditions and case outcomes.

Kamcev later initiated a civil case against the head prosecutor and others, claiming they had extorted him. A Skopje civil court ruled that Kamcev was not a victim and was not entitled to compensatory damage.

In the aftermath of the scandal, the SPO collapsed. As a result, many high-level corruption cases remain stagnant and undecided, delaying accountability for numerous individuals who have engaged in corruption similar to Kamcev.

"Moscow's Man" in Belgrade Sanctioned

► Treasury's Office of Foreign Assets Control (OFAC) imposed sanctions today on **Aleksandar Vulin**, a high-ranking Serbian official. This move comes under the Executive Order (E.O.) 14033, aiming to combat corruption within the Western Balkans.

Vulin has been associated with various illegal activities, including transnational organized crime and drug trafficking. He has been particularly highlighted for his connections with **Slobodan Tesic**, a U.S.-designated Serbian arms dealer, helping facilitate illegal arms transportation across Serbian borders.

As the Director of Serbia's Security Information Agency, and former Minister of Defense and Minister of the Interior, Vulin is accused of exploiting his official roles to further Russia's interests in the Western Balkans, negatively affecting the region's stability and security.

The Associate Press has described Vulin as "Moscow's man" within the Serbian leadership, and his outspoken support for Russia has made him few friends in the Western Defense Establishment.

OFAC implemented the sanctions in response to allegations of corruption, including misappropriation of public assets, bribery, and expropriation of private assets for personal or political gain in the Western Balkans.

It is important to note that the institutions Vulin represented are not the subjects of these sanctions.

SUPPLY CHAIN

UFLPA

Strategy Updated

THE FORCED LABOR Enforcement Task Force (FLETF) has published an updated Uyghur Forced Labor Prevention Act (UFLPA) Strategy to Prevent the Importation of Goods Mined, Produced, or Manufactured with Forced Labor in the People's Republic of China.

The UFLPA requires that the FLETF provide annual updates to the UFLPA Strategy addressing the UFLPA Entity List, the list of products associated with certain listed entities, plans for enforcement and for identifying additional entities, and high-priority sectors. The 2023 updates to the UFLPA Strategy include changes and additions to:

Chapter II. Evaluation and Description of Forced-Labor Schemes and UFLPA Entity List

Chapter V. Additional Resources Necessary to Ensure No Goods Made with Forced Labor Enter at U.S. Ports

Chapter VII. Coordination and Collaboration with Appropriate Nongovernmental Organiza-

tions and Private-Sector Entities

The updated UFLPA Strategy highlights enforcement of the UFLPA's rebuttable presumption, which prohibits goods from being imported into the United States that are either produced in Xinjiang, or by entities identified on the UFLPA Entity List, unless the importer can prove, by clear and convincing evidence, the goods were not produced with forced labor. In the first year of enforcement under the new law, U.S. Customs and Border Protection (CBP) reviewed more than 4,000 shipments valued at over \$1.3 billion.

Additionally, the strategy highlights an expanded UFLPA Entity List. Goods produced by four new companies and their subsidiaries will be restricted from entering the United States because of their work with the PRC government to recruit, transport, transfer, harbor or receive forced labor or members of persecuted groups, including Uyghur minorities, out of the Xinjiang Uyghur region.

Goods produced by the sanctioned firms include Touch Screens for Handheld Devices and Cars, Polysilicon, including Solar-Grade Polysilicon, Processed Cotton, Cotton Products and Apparel, and Polyvinyl Chloride (PVC); Chlor-Alkali Products; and Other Chemical and Textile Products.

The FLETF, chaired by the Department of Homeland Security, leads efforts to monitor implementation of the UFLPA and the broader U.S. law prohibiting the importation into the United States of goods made wholly or in part with forced labor.

In addition to the Department of Homeland Security, the FLETF is comprised of seven member agencies: the Office of the United States Trade Representative and the Departments of Labor, State, Treasury, Justice, and Commerce.

Sanctioned goods include solar-grade polysilicon.



Compliance in Solar Supply Chain

THE UYGHUR REGION PRODUCES between one third and one half of the world's solar-grade polysilicon, as well as much as 32% of global metallurgical grade silicon (MGS), polysilicon's pre-cursor material. So if it's a solar panel, the odds are good slavery had a hand making it.

Alan Crawford and Laura Murphy of Sheffield Hallam University published a review of the solar panel supply chain and its potential exposure to modern slavery, and the findings were discouraging.

“Despite significant global pressure for increased transparency, information regarding solar industry sourcing is becoming less transparent over time, thwarting the world's ability to source ethically,” the Authors write.

“Information about solar sourcing has become increasingly unavailable following the revelations of the solar industry's reliance on—and resultant complicity in—the oppression in the Uyghur Region.... Public trust in the solar industry is extremely low,”

Crawford and Murphy assessed the top five manufacturers (which together manufacture 70% of the world's solar modules), and found the vast majority of modules produced globally continues to have exposure to the Uyghur Region

The most significant findings of the report include the following:

- Companies that have created supply chains purportedly free of XUAR inputs continue to source from suppliers or sub-suppliers that have exposure to the Uyghur Region for other product lines.

- It is sometimes impossible to determine if it is indeed the case that these dedicated product lines are XUAR-input-free because companies do not disclose sufficient supply chain information.

“Though there is increasing appetite for ethical sourcing of solar modules on the part of governments, developers, and domestic consumers, there is no way for these stakeholders to easily and accurately determine whether a particular silicon-based solar module contains silicon produced with forced labor in the XUAR. The problem results from the global silicon-based solar industry's almost universal lack of transparency regarding the full supply chains of silicon-based



ADOBESTOCK

solar modules.”

The lack of transparency is amplified by a blind spot in the industry regarding the most upstream segments of the supply chain, which are mining quartz rock for conversion to MGS and producing polysilicon from the MGS

“For years, the solar industry has described its supply chain as if it begins with polysilicon, without regard to where or how the polysilicon was produced, so long as the purity/ quality was assured. It is not unusual to hear people talk about polysilicon as a “raw material” or even to read of the “mining” of polysilicon, even though that is far from the truth. This is a critical oversight because quartz mining and MGS production segments are the most likely supply chain segments to transfer Uyghur Region exposure to the entire solar supply chain.

Many companies have attempted to “bifurcate” their supply chains to comply with regulations and consumer demand, producing some product lines that include XUAR inputs and others that they claim do not.

At the same time, batches of MGS or polysilicon sourced from different locations are often blended, which could introduce XUAR-sourced materials into any batch made by a company sourcing any amount of materials from the region. Bifurcation of solar module supply chains

Continues on next page

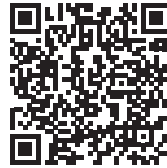
Continued from previous page

presents a significant challenge to the wide range of governments, developers, and consumers purchasing modules, as they cannot always be certain whether they are buying the tainted or untainted product

- The five named solar panel manufacturers have operations in North America. **Qcells** and **Jinko Solar**, have US operations, while **JA Solar** will produce modules in Arizona, US beginning in

late 2023. **Maxeon** and **Canadian Solar**, manufacture products just north or south of the U.S. border.

The report does not speak to the supply chains of three leading US manufacturers **First Solar**, **Silfab** and **Mission Solar**.



Scan the code to read the **Sheffield Hallam Report** or go to: exportprac.com/stories/slavery-in-solar-supply-chain-detailed,10866

House Leaders Bash Ford Sourcing Plans

IN A STERNLY WORDED LETTER to CEO **Jim Farley** of the Ford Motor Company, two of the House's leading China Hawks lashed into the company's plans to license Chinese technology for electric vehicle battery production, calling for access to Ford's business records and correspondence related to the deal.

Chairman of the House Committee on Ways and Means **Jason Smith** (R-MO) and **Rep. Mike Gallagher** (R-WI) of the Select Committee on the Chinese Communist Party asked to review all corporate and external communications relating to the licensing agreement, as well as all communications on the topic with the White House.

Chinese in Workforce

Among the objections the lawmakers cite is the intention of Ford to engage. CATL employees from the PRC to set up and maintain the licensed technology.

Supply Chain Questioned

They also note that CATL maintains extensive links to Xinjiang Lithium, a documented exploiter of Forced Labor. Ford's and

CATL's decision to trade with Xinjiang Lithium and other materials suppliers raise questions of compliance with the Uyghur Forced Labor Protection Act, as well as the project's reliance on Chinese mineral supplies.

"If Ford instead avoided iron sulfate from China and supported the development of homegrown process technologies and local sourcing strategies, it could play a central role in further developing the supply chain for North American sourced cathode active materials," the lawmakers wrote.

Deal Structure Criticized

"By entering into a licensing agreement instead of a traditional joint venture with PRC-based CATL, Ford can likely exploit the Section 30D

clean vehicle credit aimed at reducing reliance on foreign technology and labor in the design and development of American electric vehicles.

"Such behavior raises serious questions as Conas [sic] Congress conducts oversight of the implementation of this and other federal tax incentives.

Corporate Information requested

- A copy of the licensing agreement between Ford and CATL—including all appendices—in both English and Chinese;
- All documents and communications between Ford and CATL referring or relating to the licensing agreement in the original language, i.e. not in translation; and
- All documents and communications between Ford and the Biden Administration referring or relating to the Ford/CATL licensing agreement and/or achievable tax credits.



Visit the website to read the letter:



BRIEFS

Chips Defense Industrial Base Memorandum

► The Commerce and Defense Departments announced yesterday that they have signed a Memorandum of Agreement to **expand collaboration to strengthen the U.S. semiconductor defense industrial base.**

The agreement will increase information sharing between the departments to facilitate close coordination on the CHIPS for America's incentives program, ensuring that their respective investments position the United States to produce semiconductor chips essential to national security and defense programs.

The MOA is a crucial step forward in implementing the bipartisan CHIPS and Science Act, a key part of President Biden's Investing in America agenda. It will advance this agenda to strengthen manufacturing and supply chains here at home, solidify America's global leadership and protect long-term national security.

By aligning priorities and decision-making, the MOA will enable a more synchronized approach to promoting a robust and resilient semiconductor supply chain, according to the departments. Specific areas of consultation identified in the MOA include sharing information on the semiconductor needs of the Defense Industrial Base, the investment priorities of DoD and each military service, the existing and planned investments to sustain mature and legacy chip capabilities for current defense programs and funding to support emerging technologies that are critical to future US national security programs.

The agreement also will facilitate collaboration on potential investment applications to ensure Commerce and Defense are making complementary decisions that maximize federal investments under the CHIPS Incentive Program and DoD Defense Production Act and Industrial Base Analysis and Sustainment funds.



Sen. Wyden Slams 'Cattle Laundering'

► Senate Finance Committee Chair **Ron Wyden**, D-Ore., requested in a new letter that Lear Co., the nation's largest car seat manufacturer, explain how it oversees leather supply chains in Brazil to prevent the illegal importation of goods made with forced labor or deforestation. Environmental groups and journalists have documented widespread forced labor and human rights abuses at ranches sited on illegally cleared Amazon rainforest.

"These ranches evade supply chain monitoring by moving cattle repeatedly over their lifetimes from illegal to legal ranches in a process known as 'cattle laundering,'" Wyden wrote. "In addition to encouraging deforestation, illegal ranching in the Amazon drives violent land-grabs and human rights abuses, subject to weak oversight by Brazilian law enforcement, which often fails to enforce environmental and human rights laws."

The letter comes as part of Wyden's ongoing inquiry into forced labor in auto supply chains. Wyden has written to major automakers and their tier 1 suppliers regarding evidence of parts made with forced labor in Xinjiang, China, as part of his investigation into the effectiveness of customs enforcement regarding forced labor. In June, he held a Finance Committee hearing investigating how cattle supply chains contribute to Amazon deforestation.

"The information I am requesting from Lear will aid the Senate Finance Committee's investigation of the effectiveness of trade-based efforts by the United States to combat forced labor and environmental abuses in the supply chains of products sold in the United States," Wyden wrote.

Herd of zebu Nellore cattle, Brazil.

ALF RIBEIRO

```
...preventDefault()),d.isDefault...
...transitionEnd(150):c());var
...alert.constructor=d,a.fn.alert.noCon
...click.bs.alert.data-api",c,d.pro
...data("bs.button"),f="object":
...function(b,d){this.$element=a(b
...loadingText:"loading..."},c.prototy
...data();b="Text",null=f.n
...function(){loadingText==b
...loading(this.isloading=!1,d.remov
...manager.buttons"});if(b.length){va
...type)}(c.prop("checked")&&
...checked",!this
...fn.button;a.fn.button=b,a.fn
...click.bs.button.data-api",[data
...preventDefault())}(jQuer
...extend({},c.DEFAULTS,d.data(),
...=typeof b?e.to(b):g?e
...prop(this.keydown,this)),t
...this.sliding=this.interval=t
...prop(this.pause,this)).on("m
...this.prototype.keydown=function(a
...preventDefault()),c.prototype.c
...this.interval,this.options.interval&
...prop(this.next,this),this.
...this.items.index(a||this.$active
...);return b>this.$items.leng
...to(b));d=b?this.pause(
...return b||(this.pause
```