


EP IN

THE EXPORT PRACTITIONER™

THIS ISSUE:

- ▶ Uyghur Audits “Fig Leaf”
- ▶ Individual Self-Disclosure
- ▶ AUKUS Updates to ITAR & EAR
- ▶ Sanctions Lookback now 10 Years



Steel Deal Brings CFIUS Up Front

Inside: Auditors Cheating, More Car Wash, May Day Sanctions

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.

Scan or
Click For Our
Top Stories:



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

Contact Editor Frank Ruffing at
fruffing@traderegs.com,
or call 703-283-5220.

VISIT ONLINE AT
EXPORTPRAC.COM

EP

THE EXPORT PRACTITIONER™

May 2024 | VOL. 38, NO. 5



ADOBESTOCK/TAITAI6769

FEATURE

- U.S. Steel:** Nippon Steel Sale Under Siege | 4
- CFIUS Rules** Sharpened and Enhanced | 5
- CFIUS Report:** Volume growth calls for reform | 6

POLICY

- Uyghur Audits:** an “unreliable fig leaf” | 8
- China Committee:** New Chair Steps up | 9
- Wall Street:** China Investment slammed | 9
- Biotech:** Calls for regulation of Chinese | 10
- Export Controls:** Senate calls for coordination | 11
- Briefs:** TTC, AI, FATF, EU AML, Puerto Rico | 12
- Self Disclosure:** Pilot announced | 13

EXPORT CONTROLS

- AUKUS:** State issues ITAR Rules | 14
- AUKUS:** Commerce issues EAR Exemptions | 16
- Firearms Licensing:** Commerce ends “pause” | 17
- Briefs:** FDP rule scope, Medical Devices, DDTC | 18

SANCTIONS

- May Day Sanctions:** 300 targeted | 20
- Briefs:** EU Rules, Metals Trading, Adeyemo | 21
- PRC sanctions** US firms, Belarus, Iran, DPRK | 21

ENFORCEMENT

- KPMG Fined:** “inappropriate tone at top” | 23
- Chipmaking Equipment:** PRC agents nabbed | 24
- Iran Sanctions:** \$20 million fine for Thai firm | 24
- Venezuela:** Executive jet fleet arrest | 25
- Russian Airlines:** MRO Support plea | 26
- Russian Steel:** Florida trader gets six years | 27
- Ecuador:** Former official convicted | 28
- CITES:** Handbag maker sentenced | 28

SUPPLY CHAIN

- EU Forced Labor:** Legislation “toothless” | 29
- Textiles:** Customs & HSI up enforcement | 30
- USMCA Briefs:** Mexico wins on jurisdiction; call centers, Japan-Mexico JV targeted. | 31

ON THE COVER: Molten steel. ADOBESTOCK / MIRACLE MOMENTS

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 2024 Gilston-Kalin Communications, LLC
ISSN 1087-478K



Employees working at the U. S. Steel Gary Works pig iron caster.

U.S. STEEL

CFIUS

U.S. Steel Sale to Japanese Under Siege

It is premature to declare Nippon Steel’s bid to buy U.S. Steel dead, despite election year politics driving acerbic scrutiny from Labor and legislators.

April 17 President Biden told a crowd in Pittsburgh that U.S. Steel “has been an iconic American company for more than a century and it should remain totally American,” and saying it was “vital for it to remain an American steel company that is domestically owned and operated.”

“American-owned, American-operated by American union steelworkers — the best in the world — and that’s going to happen, I promise you,” he told the crowd.

“The partnership between U.S. Steel and Nippon Steel is the right combination to ensure that U.S. Steel remains an iconic American company

for generations to come,” the steelmakers said in a joint statement. “Its iconic name will be unchanged, and its products will remain mined, melted and made in America,”

The United Steelworkers continue to scoff at Nippon Steel’s overtures, calling them “nothing more than another collection of empty promises and

open-ended language that would enable it to skirt obligations to workers and retirees.

Nippon Steel had sent a letter to the U.S.W on

March 27 in its attempt to gain union support for its proposed purchase of U.S. Steel. According to the U.S.W, the letter was “another meaningless piece of paper.”

Ohio Democratic **Sen. Sherrod Brown** is urging President Biden to examine the relationship between Nippon Steel and the Chinese steel industry as the company seeks to buy U.S. Steel. In a letter to the President, Sen. Brown pointed to a new report from geopolitical and risk intelligence provider **Horizon Advisory** that details the longstanding relationship between Nippon Steel and the Chinese steel industry and the dangers it could pose to U.S. national and economic security.

The proposed sale of U.S. Steel to Nippon currently is under review by the inter-agency Committee on Foreign Investment (CFIUS) in the United States to determine whether there are any potential national security risks. Bloomberg reports the Steelworkers Union is promoting national defense concerns that the replacement of blast furnaces with electric arc plants could restrict military-grade steel production.

“As you examine this deal, I urge you to thoroughly investigate the allegations raised in this report and examine Nippon’s ties to the Chinese government and the danger this merger poses to American national and economic security,” Sen. Brown wrote. “We cannot allow our U.S. industrial base to be compromised through further entanglement with one of our biggest national security threats, and our largest economic competitor that

we know does not follow our trade laws.”

Sen. Brown chairs the Senate Banking Committee and is a member of the Finance Committee. He is up for reelection this November in a tight race. Should the Nippon acquisition be derailed, constituent steelmaker Cleveland-Cliffs has proposed buying U.S. Steel for 45 percent less, though antitrust hurdles would be profound.

Japan is the United State’s leading source of foreign direct investment, with more than 900,000 Americans employed at U.S. subsidiaries and affiliates of Japanese companies. Over 73,000 Ohioans are employed by 860 Japanese companies, including Honda Motor Co., Ltd. Bridgestone Corporation, and Fujitec Co., Ltd. [\[12127\]](#)

Carrie Furnace, Homestead, PA.

BILL DICKINSON (CC BY-NC-ND 2.0)



CFIUS Rules ‘Sharpened and Enhanced’

The Treasury Department, as Chair of the Committee on Foreign Investment in the United States (CFIUS), issued a Notice of Proposed Rulemaking (NPRM) to “enhance certain CFIUS procedures and sharpen its penalty and enforcement authorities.”

The proposed rule reflects CFIUS’s first substantive update to the mitigation and enforcement provisions of the CFIUS regulations since the enactment

and implementation of the Foreign Investment Risk Review Modernization Act of 2018, which amended CFIUS’s governing statute (section 721 of the Defense Production Act of 1950).

The rule “hones “ CFIUS’s ability to accomplish its national security mission consistent with the United States’ open investment policy, according to a Treasury Department statement.

CFIUS is authorized to review cer-

tain transactions involving foreign investment into businesses in the United States and certain transactions by foreign persons involving real estate in the United States in order to determine the effect of such transactions on the national security of the United States.

CFIUS enforces transaction parties’ compliance with its statute and regulations, as well as agreements entered

Continues on next page

Continued from previous page

into and conditions and orders imposed under such authorities, through its authority to impose civil monetary penalties and seek other remedies.

• **The proposed rule would refine and enhance CFIUS's authorities through the following key changes:**

• **Expanding the types of information CFIUS can require transaction parties and other persons to submit** when engaging

with them on transactions that were not filed with CFIUS;

• **Instituting an extendable timeline** for transaction parties to respond to risk mitigation proposals for matters under active review to assist CFIUS in concluding its reviews and investigations within the statutory time frame;



• **Expanding the circumstances in which a civil monetary penalty may be imposed due to a party's material misstatement and omission**, including when the material misstatement or omission occurs outside a review or investigation of a transaction and when it occurs in the context of the Committee's monitoring and compliance functions;

• **Substantially increasing the maximum civil monetary penalty available** for violations of obligations under the CFIUS statute and regulations, as well as agreements, orders, and conditions authorized by the statute and regulations, and introducing a new method for determining the maximum possible penalty for a breach of a mitigation agreement, condition, or order imposed;

• **Expanding the instances in which CFIUS**

may use its subpoena authority, including when seeking to obtain information from third persons not party to a transaction notified to CFIUS and in connection with assessing national security risk associated with non-notified transactions; and

• **Extending the time frame for submission of a petition for reconsideration of a penalty** to the Committee and the number of days for the Committee to respond to such a petition.

“As CFIUS has refined its focus on compliance and enforcement, we've identified important enhancements to our regulations to more effectively deter violations, promote compliance, and swiftly address national security risks in connection with CFIUS reviews,” said **Assistant Secretary for Investment Security Paul Rosen**. [\[12032\]](#)

GAO REPORT

CFIUS Volume Growth Calls for Reforms

The Committee on Foreign Investment in the United States (CFIUS) has seen explosive caseload in recent years, though a performance audit finds the committee organization and management has struggled to keep up, according to a report released by the General Accounting Office (GAO).

Since 2000, the number of mitigation agreements has steadily increased, approximately quadrupling in the last decade, managed predominantly by the Departments of Defense and the Treasury. From December 2000 to December 2022, the total number of active mitigation agreements rose significantly from approximately five to nearly 230, reflecting an accumulation of ongoing agreements and the signing of new ones.

Staffing Concerns

The report notes that the increasing number and complexity of foreign investment transactions reviewed by CFIUS raises **concerns about its capability to effectively monitor and enforce compliance with these agreements**.

The report also underscores challenges within CFIUS including **an absence of documented processes** for achieving consensus on enforcement actions

or for deciding when to terminate outdated mitigation agreements.

Treasury plans to double its CFIUS monitoring staff by the end of fiscal year 2024 but has not documented objectives for this expansion, basing it on estimates rather than assessed needs.

Officials from the five selected agencies for the review pointed to an increase in both the number and complexity of mitigation agreements, questioning their capacity to sustain effective oversight.

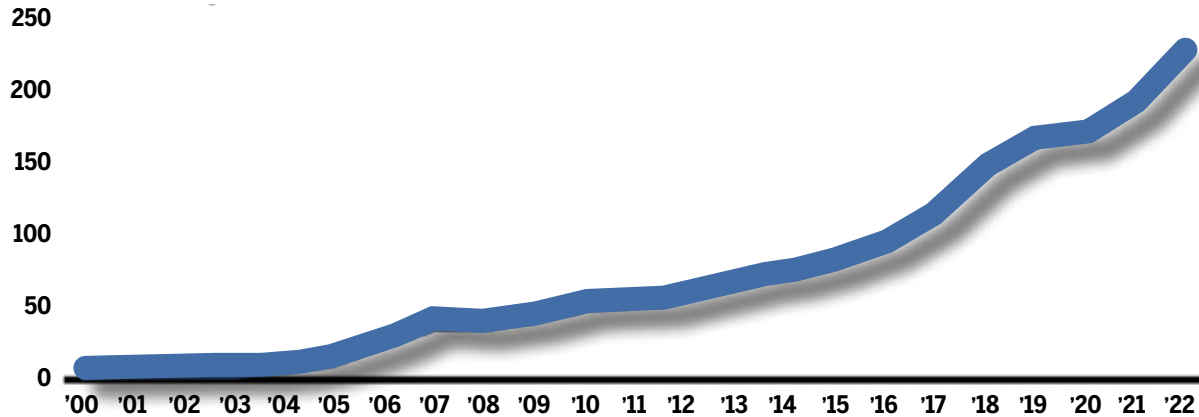
Monitoring and Enforcement

The report evaluates trends in mitigation agreements from 2000 through 2022, assesses approaches to monitoring, enforcing compliance, and reviewing the continued relevance of these agreements by selected CFIUS member agencies, and examines these agencies' staffing for monitoring and enforcement.

Officials from three of the five selected agencies expressed that their current resource levels are inadequate to meet or expand the scope of their monitoring and enforcement efforts. Although site visits are deemed essential for monitoring some agreements, officials from two agencies reported

Number of Active CFIUS Mitigation Agreements, by Calendar Year, 2000–2022

Total number of agreements



SOURCE: GAO analysis of Dept. of the Treasury data on the CFIUS in the U.S. | GAO-24-107358

insufficient resources to meet site visit targets.

Despite shared responsibilities, CFIUS does not regularly discuss or coordinate on necessary staffing levels to monitor and enforce compliance with mitigation agreements. The Treasury, as CFIUS’s chair, has not established a regular, committee-wide process for discussing and coordinating staffing needs among members.

Enforcement Challenges

Furthermore, CFIUS lacks a documented committee-wide process for deciding on enforcement actions, leading to challenges in addressing violations. Officials noted that each enforcement action is context-specific, which complicates the establishment of general criteria for enforcement.

Recommendations:

- The Secretary of the Treasury, as Chair of CFIUS, should collaborate with member agencies to establish and document a committee-wide procedure for considering and executing timely enforcement actions related to mitigation agreements.
- The Secretary of the Treasury, as Chair of CFIUS, should initiate the documentation of a committee-wide process that periodically assesses the relevance of mitigation agreements and, where appropriate, amends, phases out, or terminates them.
- The Secretary of the Treasury should formally record Treasury’s goals for the planned increase in staff dedicated to monitoring and enforcing compliance with CFIUS mitigation agreements.
- Once the targeted staffing increase is achieved, the Secretary of the Treasury should evaluate

Treasury’s CFIUS monitoring and enforcement staffing in accordance with federal workforce planning guidelines to ascertain whether the increase has enabled Treasury to meet its documented objectives.

- The Secretary of the Treasury, as Chair of CFIUS, should facilitate the establishment of a regular, committee-wide dialogue among member agencies to discuss and coordinate necessary staffing levels in response to the anticipated rise in workload linked to the monitoring and enforcement of CFIUS mitigation agreements. [\[12088\]](#)

Examples of National Security Risks Addressed by CFIUS Mitigation Agreements



Supply assurance and product integrity

The risk that the foreign acquisition will compromise the supply or performance of a critical good or service the U.S. government buys



Data and information security

The risk that the foreign acquisition will enable access to certain data or information that will compromise national security



Proximity concerns

The risk that a foreign acquisition’s close proximity to, or colocation with, a sensitive facility, such as a military installation, will compromise national security



Technology transfer

The risk that a foreign acquisition will transfer or enable access to sensitive intellectual property, trade secrets, or other technological know-how

SOURCE: CFIUS documents, GAO icons. | GAO-107358

CHINA COMMITTEES

Uyghur Compliance Audits Unreliable ‘Fig Leaf’

U.S. businesses with suppliers located in China’s Xinjiang region cannot rely on social audits to confirm whether forced labor is being used in their supply chains, a top Administration labor official told lawmakers in an April 30 hearing.

“Social audits in China should not be seen as an authoritative source for companies reflecting on-the-ground human rights conditions,” **Deputy Undersecretary of Labor for International Affairs Thea Lee** said.

“The business community needs to be aware that any audits, and frankly any business operations undertaken inside China, carry heightened labor and human rights risks,” she told members of the Congressional Executive Commission on China at a hearing on audit fraud.

The audits are required under the Uyghur Forced Labor Prevention Act to ensure that products made with forced labor are not finding their way into U.S. supply chains. But the reliability of such audits are questionable, Ms. Lee said.

Reprisals Feared

“Any audit occurring in Xinjiang cannot be conducted without government oversight, making objective worker interviews free from reprisal an impossibility,” she said.

“As the U.S. government highlighted in the Xinjiang Business Advisory2F3, published in 2021 and updated in September of 2023, auditor interviews with workers cannot be relied upon given pervasive surveillance, the threat of detainment, and evidence of workers’ fear of sharing accurate information.

“Moreover, auditors have reportedly been detained, harassed, threatened, or stopped at the airport. That is why dozens of major audit firms have not operated in Xinjiang for years; the fear of reprisal for both workers and auditors remains high.”

Committee co-chair **Rep. Chris Smith** (R-NJ) agreed. “Today, using the fig leaf that audits provide, corporations seek to convince consumers, regulators and perhaps even their own consciences that their supply chains are clean and compliant with U.S. law,” he said.



ADOBESTOCK / DIDIER

Uyghur women near shops in Kashgar, Xinjiang, China. Auditor interviews with workers in the region cannot be relied upon given pervasive surveillance.

Rep. Smith said he intends to hold an additional hearing with audit companies. He is hoping to receive input on what regulatory or legislative actions Congress might need to take.

The Administration and Congress had hoped the UFLPA would persuade China to end the practice of forced labor and human rights abuses of the Uyghur ethnic minority, but Beijing has not budged, Ms. Lee said. With other countries, including the European Union, adopting similar measures, hopefully at some point it will become untenable for China to continue its actions.

New Chair Makes Noise

The New Chairman of the House Select Committee on the Strategic Competition between the United States and the Chinese Communist Party, **Rep. John Moolenaar** (R-MI) promises to continue the Committee's role as a spotlight, though arguably with less candlepower than his predecessor, retiring **Rep. Mike Gallagher** (R-WI).

In a series of press statements, Mr. Moolenaar plowed familiar ground.

"**Gotion** is trying to build a battery component factory in my district, and numerous concerns have been raised over the past year and half," he wrote, referring to plans to build a \$2.4 billion battery plant that Democratic Gov. Gretchen Whitmer has called "the biggest ever economic development project in northern Michigan." The China-based company's largest shareholder is Volkswagen Group and the board is one-third German, one-third American and one-third Chinese. [11093]

"Traveling overseas and crisscrossing the country as a member of the Committee, from the Pacific coast of California to the industrial centers in my home state of Michigan, I've witnessed the CCP's near-constant efforts to undermine America's core values and sovereignty," Mr. Moolenaar said in a statement.

"Just look at the CCP's use of TikTok to indoctrinate our children, their efforts to buy our farmland, and the secret police stations the Chinese government has directed and operated right here on U.S. soil. "The CCP is actively targeting all facets of American life, including our economy, national

security, and even the privacy of our own homes."

"From my time working on the Select Committee I have come to understand that what the Chinese Communist Party really fears most is a united America; an America where Democrats and Republicans work together to defend our nation."

Thin Background

The former Dow Chemical Chemist has represented the rural Michigan district since the 2014 retirement of former Republican **Ways & Means Chairman Dave Camp**. In addition to the CCP Committee, Mr. Moolenaar sits on the Appropriations Committee, where his work has focused on agriculture, rural development, and education.

Unlike former Chairman Mike Gallagher, Mr. Moolenaar has no military or foreign policy experience. In addition to voting earlier this year to impeach DHS Secretary Alejandro Mayorkas, Mr. Moolenaar signed an amicus brief before the U.S. Supreme Court in *Texas v. Pennsylvania, et. al.*, seeking to overturn the 2020 U.S. presidential election results.



"The CCP is actively targeting all facets of American life, including our economy, national security, and even the privacy of our own homes."

REP. JOHN MOOLENAAR

Index Providers Slammed

A report from the House Select Committee on China found that U.S. financial institutions have facilitated investment of more than \$6.5 billion to 63 Chinese companies that the U.S. government has red-flagged or blacklisted for advancing Beijing's military capabilities or supporting its human rights abuses.

Their bipartisan investigation examined the world's foremost index provider, MSCI, and the world's largest asset

manager, BlackRock. The investigation also included a canvass of the broader U.S. financial industry.

According to their findings, U.S. financial institutions are "facilitating investments worth billions of dollars in Chinese companies that advance the country's military ambitions and perpetrate human rights abuses."

Findings

In 2023, according to the report:

Major financial institutions provided \$6.5 billion to 63 PRC companies that the U.S. government has blacklisted or otherwise red-flagged because they

advance the PRC's military capabilities or support the CCP's human rights abuses.

MSCI indexes alone channeled \$3.7 billion to these entities.

BlackRock invested at least \$1.9 billion in these companies.

Congressional Action

"What may surprise many Americans is that the activity by U.S. financial institutions described ...is not illegal. It is time for Congress to act," the lawmakers said. "The existing regulations prohibiting investment in **Continues on next page**

Continued from previous page

certain Chinese companies because of national security risks or human rights violations are insufficient,” they said. “Congress must act to restrict U.S. investment in entities tied, directly or in-

directly, to the PLA, critical technology sectors, or forced labor and genocide.”

According to the lawmakers, Congress specifically should pass legislation to:

Restrict investment in companies blacklisted by the U.S. government, in-

cluding subsidiaries, affiliates, parents and holding companies.

Require U.S. public companies to “disclose key risks related to the PRC.”

Ensure the U.S. financial system is “resilient to PRC market uncertainty.” [\[12083\]](#)

Complete Genomics headquarters in Silicon Valley; Complete Genomics Inc is a life sciences company owned by BGI-Shenzhen

ADOBESTOCK / SUNDRY PHOTOGRAPHY



Chinese Biotech Targeted

The leaders of the House Select Committee on China are warning that a Chinese military company, BGI, is attempting to set up a new firm, Innomics, in Massachusetts and Kentucky, to avoid U.S. regulatory scrutiny.

In a letter to Defense Secretary Lloyd Austin, Committee Chairman Mike Gallagher (R-Wisc) and ranking Democrat Raja Krishnamoorthi (Ill) urged the Pentagon to label Chinese companies that aid the Chinese Communist Party in military biotech research as “Chinese Military Companies.”

“The PRC’s 14th Five-Year Plan identifies dominance in biotechnology as critical to ‘strengthen the PRC’s science and technological power’ and calls to deepen military-civil science and technology collaboration in the sector,” the lawmakers wrote.

“PRC military and academic literature further stresses the importance of biotechnology to national power, arguing success on the future battlefield

will require ‘achieving biological dominance,’ with one former president of the People’s Liberation Army’s (PLA) National Defense University openly discussing biotech’s ability to create synthetic pathogens that are ‘more toxic, more contagious, and more resistant.’ Urgent action is needed to identify the PRC biotechnology entities at the forefront of this work.”

They called on the Pentagon to consider labeling the following biotech companies ‘Chinese Military Companies’: MGI Group and Complete Genomics, Innomics and STOmics, Origincell, Vazyme Biotech and Axbio.

Section 1312 of the National Defense Authorization Act for Fiscal Year 2024 requires Defense to identify and place problematic People’s Republic of China biotechnology companies on the DoD’s 1260H list of Chinese Military Companies within 180 days. [\[12009\]](#)

SENATE

Focus on Export Enforcement

Senators **Mitt Romney** (R-UT) and **Maggie Hassan** (D-NH) have introduced bipartisan legislation intended to improve export controls enforcement. The Export Controls Enforcement Improvement Act bolsters the **Export Enforcement Coordination Center** — an interagency hub for information sharing and coordination among the key agencies responsible for export control enforcement.

The *Export Controls Enforcement Improvement Act* would:

- Formally establish and promote consistent staffing levels for the Export Enforcement Coordination Center (E2C2).

- Target and focus enforcement efforts on critical matters for national security:

- The unlawful transshipment and diversion of exports to China, Russia, Iran, and North Korea; and

- Sensitive technologies involving semiconductors, artificial intelligence, and quantum technology.

- Require an assessment of the value of increasing the number of law enforcement officials posted in foreign countries focused on export controls.

- Support coordination with the private sector to ensure U.S. companies are aware of latest threats and risks of transshipment.

Subcommittee Hearing

As Ranking Member and Chair of the Senate Homeland Security & Governmental Affairs (HS-GAC) Emerging Threats and Spending Oversight (ETSO) Subcommittee respectively, Senators Romney and Hansen held a hearing April 10 promoting their legislation.

“This Center should be the heartbeat for export controls coordination. Our legislation would help ensure that agencies are talking to each other and working with the private sector and foreign partners to keep sensitive technologies from going to U.S. adversaries, said Sen. Romney.

Witnesses included **James Mancuso**, Assistant Director, Global Trade and Investigations Division, Homeland Security Investigation. “We are the envy of the entire world. That also means our adversaries will stop at nothing to obtain this technology in these weapon systems... We are an investigative agency looking at these agencies attempting to



disrupt and dismantle the flow of this technology,” said Mancuso. “I’m also concerned the day that they don’t want our technology, that day that we aren’t the world leader, because that means that they’ve surpassed us and they’ve become superior. And all of us at this table are laser focused on making sure that day never happens.”

Deputy Assistant Attorney General in the National Security Division **Eun Young Choi** called for more support from Congress. “We simply are at our wit’s end when it comes to resourcing and doing the big data analytics. And we know our adversaries are dealing with our data. We need to be able to do that and be armed to do that. And so I would have that in mind when you’re thinking about resourcing in the FY25.

“**One other thing that’s maybe not so obvious but is very important to us is the reauthorization of Section 702.** It’s absolutely vital to all of the national security work that we do. But in particular, I think it’s important to highlight that in certain instances we’ve been able to glean insights into illicit transfer of technology and goods to hostile foreign state actors through the use of that particular tool.”

Deputy Assistant Secretary of Commerce for Export Enforcement **Kevin Kurland** repeated his fellow witnesses call for resources. “I’m on the enforcement side but what I can commit to you is

Continues on next page

Sen Maggie Hansen (D-NH)

Continued from previous page

that if new actions are taken, we will commit to aggressively enforce those. From our perspective, you know, that requires more analysts, more attachés overseas, more agents that are working with DOJ to bring criminal cases.

“And it gets back to that IT issue as well: better IT systems so that we can create efficiencies to identify these violators and then more quickly be able to bring those cases, whether it’s a criminal case, whether it’s an administrative case, whether

it’s an entity listing...But the more resources that we have, the more effective we can be.”

Call for Audit

In January, Senators Romney and Hassan sent a letter to the Government Accountability Office (GAO) requesting an assessment of the Department of Commerce’s export controls restricting advanced semiconductors, semiconductor manufacturing equipment, and related technologies from going to China and other adversaries. [\[12035\]](#)

Our legislation would help ensure that agencies are talking to each other and working with the private sector and foreign partners to keep sensitive technologies from going to U.S. adversaries

Sen. Mitt Romney.

BRIEFS

TTC Ministerial Yields Little

► The United States and European Union Trade and Technology Council (TTC) Ministerial meeting April 4 discussed “Approaches to decarbonization that protect and center workers and workers’ rights” according to U.S. Trade Representative Katherine Tai, though the joint ministerial readout on the overall TTC meeting failed to mention substantive progress on alignment of Carbon Tax policies of the parties. [\[12022\]](#)

TTC Aims at Artificial Intelligence

► The ministers reaffirmed their common commitment to a “risk-based approach” to artificial intelligence, including a new dialogue between the EU AI office and the U.S. Safety Institute on developing tools, methodologies, and benchmarks for measuring and evaluating AI models. Specific areas of discussion included Post Quantum Cryptography (PQC), a “Common 6G Vision,” and semiconductor supply chain collaboration. [\[12008\]](#)

U.S. UK AI Safety Pact Inked

► The U.S. and UK signed a Memorandum of Understanding (MOU) which will see them work together to develop tests for the most advanced AI models, following through on commitments made at the AI

Safety Summit last November. The U.S. and UK AI Safety Institutes have laid out plans to build a common approach to AI safety testing and to share their capabilities to ensure these risks can be tackled effectively. [\[12016\]](#)

FATF Ministerial in Washington

► During their biennial meeting in Washington, DC ministers of the Financial Action Task Force (FATF) reaffirmed their commitment to combat financial crime, and fully support the FATF as the standard-setter for preventing and combating money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction (AML/CFT/CPF). Ministers highlighted the threat posed by the proliferation of weapons of mass destruction (WMD) to international peace and security. [\[12067\]](#)

EU Money Laundering Rules Update

► The European Parliament has adopted a package of laws strengthening the EU’s toolkit to fight money-laundering and terrorist financing. The new laws include enhanced due diligence measures and checks on customers’ identity, as well as an EU-wide limit of EUR 10 000 on cash payments, except between private individuals in a non-professional context, and measures to

ensure compliance with targeted financial sanctions and avoid sanctions being circumvented. [\[12111\]](#)

Puerto Rico Mission Highlights AML Risks in Commonwealth

► Under Secretary for Terrorism and Financial Intelligence (TFI) Brian Nelson travelled to San Juan, Puerto Rico for meetings with federal law enforcement partners on counternarcotics trafficking, as well as government officials and leaders from the commercial banking sector. Mr. Nelson’s visit follows FinCEN Director **Andrea Gacki**’s travel to the island in February, highlighting the increased risks in Puerto Rico due to loosely regulated Puerto Rican financial entities, (PRFEs) chartered and licensed by territorial authorities. [\[12092\]](#)



ADOBESTOCK/MARTA

The capitol building in San Juan, Puerto Rico.

Individual Self Disclosure Pilot Announced

Principal Deputy Assistant Attorney General **Nicole M. Argentieri**, head of the Justice Department's Criminal Division announced the outlines of a voluntary self-disclosure program in a statement April 22.

“Our experience shows that individuals who are involved in criminal conduct and are willing to accept responsibility and cooperate with us are critical sources of information. To provide clear incentives and encourage individuals to come forward, earlier this week I announced a new Criminal Division pilot program on voluntary self-disclosures for individuals.

“Under this pilot program, individuals with criminal exposure — *not including CEOs, CFOs, high-level foreign officials, domestic officials at any level, or individuals who organized or led the criminal scheme* — who come forward and report misconduct that was otherwise unknown to the department will be eligible to receive a non-prosecution agreement (NPA) if they meet certain criteria.

Under the new program, culpable individuals will receive an NPA if they

- voluntarily,
- truthfully, and
- completely self-disclose original information regarding misconduct that was unknown to the department in certain high-priority enforcement areas,
 - fully cooperate and are able to provide substantial assistance against those equally or more culpable, and
 - forfeit any ill-gotten gains and compensate victims.

The pilot program seeks disclosures in certain core enforcement areas for the Criminal Division, and in particular for our Fraud Section, our Money Laundering and Asset Recovery Section, and our Public Integrity Section. **Specifically, the program is open to individuals who provide disclosures involving the following:**

- Schemes involving financial institutions — including money laundering and criminal compliance-related schemes;
- Schemes related to the integrity of financial markets involving financial institutions, investment advisors or funds, or public or large private companies;

‘NPAs will not be available under the program for individuals who have engaged in certain types of criminal conduct or who have prior felony convictions or any conviction involving fraud or dishonesty.’



NICOLE M. ARGENTIERI, head of the DOJ's Criminal Division

- Foreign corruption schemes, including violations of the Foreign Corrupt Practices Act, Foreign Extortion Prevention Act, and associated money laundering;

- Health care fraud and kickback schemes;
- Federal contract fraud schemes; and
- Domestic corruption schemes involving bribes or kickbacks paid by or through public or private companies.

“In addition, as in our Corporate Enforcement Policy, the individual’s self-disclosure must be to the Criminal Division, and it must be voluntary. This means the disclosure must happen in the absence of any government investigation, before the department or any federal law enforcement, regulatory, or civil enforcement agency makes a request related to the subject matter of the disclosure, and before the threat of imminent disclosure to the government or the public.

“Also, the individual must not have a preexisting obligation to report the information to the department or any federal law enforcement, regulatory, or civil enforcement agency pursuant to a plea agreement, NPA, or similar agreement.

“As with any other program, there are some disqualifications. NPAs will not be available under the program for individuals who have engaged in certain types of criminal conduct or who have prior felony convictions or any conviction involving fraud or dishonesty.

We have a web page dedicated to this pilot program that tells you how it works.

“This individual voluntary self-disclosure pilot program will reinforce our existing corporate voluntary self-disclosure program and our developing whistleblower program, helping to expose criminal schemes. [\[12096\]](#)

EXPORT CONTROLS



AUKUS

State Issues ITAR Rules

Following on the Commerce Department’s modification of dual-use export controls for alliance partners [below], the U.S. Department of State proposes to amend the International Traffic in Arms Regulations (ITAR) to support the goals of the AUKUS partnership.

State will include an exemption to the requirement to obtain a license or other approval from the Department’s Directorate of Defense Trade Controls (DDTC) prior to any

- export, reexport, retransfer, or temporary import of defense articles;
- the performance of defense services;
- or engagement in brokering activities between or among authorized users within Australia, the United Kingdom, and the United States.

The Department also proposes to

- add a list of defense articles and defense services excluded from eligibility for transfer under the proposed new exemption.
- add to the scope of the exemption for intra-company, intra-organization, and intra-governmental transfers to allow for the transfer of classified defense articles to certain dual nationals who

are authorized users or regular employees of an authorized user within the United Kingdom and Australia; and

- revise the section on expediting license review applications by referencing new processes for Australia, the United Kingdom, and Canada.

Legislative Background

On December 22, 2023, President Biden signed the National Defense Authorization Act (“NDAA”) for Fiscal Year 2024, Public Law No. 118-31, which, among other matters, established new authorities and requirements relating to defense trade between or among Australia, the United Kingdom, and the United States. These new authorities and requirements are contained in section 1343 of the NDAA for Fiscal Year 2024, which created a new section 38(l) in the Arms Export Control Act (AECA) (22 U.S.C. 2778(l)).

Certain of these requirements include a determination and certification as to whether Australia and the United Kingdom have implemented systems of export controls that are comparable to those of the United States in several specified areas.

- If one or both partner nation’s systems are determined and certified to meet the listed standards related to export controls in the AECA, and
- if the partner nation has implemented a comparable exemption from its export controls for the

United States,

the Department would immediately implement an ITAR exemption, subject to certain statutory limitations, for the partner nation(s) to which the positive certification applies.

ITAR Changes

The proposed new exemption, designed to implement the provisions of new section 38(l) of the AECA, would be located in ITAR § 126.7 and would provide that no license or other approval is required for

- the export, reexport, retransfer, or temporary import of defense articles;
- the performance of defense services;
- or engagement in brokering activities between or among designated authorized users within Australia, the United Kingdom, and the United States, provided certain requirements and limitations are met.

These include a list of excluded defense articles and defense services not eligible for the exemption, which can be found in a proposed new Supplement No. 2 to Part 126.

The scope of excluded defense articles and defense services remain subject to revision and the Department welcomes comment. Further details regarding the requirements and limitations of the proposed exemption are as follows:

- In § 126.7(b)(1), the exemption may only be used for transfers to or within the physical territory of Australia, the United Kingdom, or the United States, per AECA section 38(l)(1)(C)(2).
- In § 126.7(b)(2), the pool of eligible members, known as authorized users, is created to facilitate secure defense trade and cooperation.
- Australia and the United Kingdom's members will undergo an authorized user enrollment process, in coordination with DDTC, and those members will be listed through the DDTC website.
- Members located in the United States must be registered with DDTC and not debarred under ITAR § 127.7.
- The UK and Australia authorized users may request that DDTC provide confirmation of the status of U.S. authorized users.

As these lists are subject to change, DDTC will confirm the eligibility of parties under this exemption prior to the transfer (e.g., export, temporary import, reexport, etc.) of defense articles or defense services.

In § 126.7(b)(3), the defense articles and defense services listed in Supplement No. 2 to Part 126 are

not eligible for this proposed exemption. These items are excluded from eligibility under the proposed exemption because

- they are exempted from eligibility by statute, including AECA section 38(j)(1)(C)(ii), or
- are specifically exempted by either the UK, Australia, or the United States, per AECA section 38(l)(4)(A).

These items are, however, subject to the expedited licensing procedures listed in § 126.15 and may be reviewed and revised during the lifetime of the exemption. The Department notes that Supplement No. 2 to Part 126 lists the U.S.ML entries in column 1 that represent the location of the excluded defense articles and defense services within the U.S.ML. A U.S.ML category's listing in column 1 does not indicate the entire U.S.ML category is excluded; only the portions of those entries that are further described in column 2 are excluded.

When reviewing the list of exclusions, careful review of all relevant entries is required. For example, when determining whether manufacturing know-how and source code described in U.S.ML Category IV(i) is excluded, entries such as exclusions for technical data designated as Missile Technology (MT) or directly related to anti-tamper articles may apply, and manufacturing know-how and source code are each addressed in separate exclusion entries:

Dual Nationals Exemption

The Department is also proposing to add a provision to the exemption in ITAR § 126.18 to allow certain dual nationals of Australia and the United Kingdom to receive classified defense articles without a separate license from DDTC.

These persons must be

- authorized users of the exemption in § 126.7 or regular employees of such authorized users in § 126.7,
- hold a security clearance approved by Australia, the United Kingdom, or the United States that is equivalent to the classification level of SECRET or above in the United States, and be located within the physical territory of Australia, the United Kingdom, or the United States or
- be a member of the armed forces of Australia, the United Kingdom, or the United States acting in their official capacity.

The proposed addition of § 126.18(e) is to facilitate the use of the exemption at § 126.7 and allow dual nationals of another country, and Australia or the

Continues on next page

Continued from previous page

United Kingdom, to transfer classified defense articles provided the listed criteria, as described in § 126.18(e), are met.

Lastly, the Department is proposing to revise § 126.15 per the provisions of section 1344 of the NDAA for Fiscal Year 2024. This revised text would note the review of license applications for exports of certain commercial, advanced-technology defense articles and defense services to or between the physical territories of Australia, the United Kingdom, or Canada, and are with government or corporate

entities from such countries, **shall be processed within certain timeframes.**

The subject export must not be eligible for transfer under an ITAR exemption. License requests related to a government-to-government agreement between Australia, the United Kingdom, or Canada and the United States must be approved, returned, or denied within 30 days of submission.

For all other license applications subject to this section, any review shall be completed no later than 45 calendar days after the date of the application. [12129]

Commerce Issues EAR Exemptions

Bureau of Industry and Security (BIS) published an interim final rule significantly reducing licensing requirements for Australia and the United Kingdom (UK) to foster defense trade and technological innovation. BIS anticipates these changes will reduce licensing burdens for trade with Australia and the UK by over 1,800 total licenses valued at over \$7.5 billion per year.

BIS is removing Commerce Control List (CCL) license requirements to allow Commerce-controlled military items, missile technology-related items,

and hot section engine-related items to be exported or reexported to Australia and the UK without a license. As a result, many Commerce-controlled items, including certain satellite-related items, will now be eligible for export or reexport to Australia and the UK without a license.

“Australia and the United Kingdom are among our closest and most longstanding allies. Our nations have robust collective security arrangements and have fought side-by-side for over a hundred years,” said Alan Estevez, Under Secretary of Commerce for Industry and Security. “BIS is taking action today to advance the AUKUS partnership by using export control authorities to support defense trade and innovation with Australia and the UK.”

Background

The AUKUS Enhanced Trilateral Security Partnership, launched in 2021, is a collaborative multinational effort between the United States, the UK, and Australia with the goals of (1) supporting collective security and defense interests, (2) deepening information and technology sharing, and (3) fostering integration of security and defense-related science, technology, industrial bases, and supply chains.

Both countries have robust export control systems and have taken additional steps in recent months to enhance technology protection. The UK’s National Security Act 2023 provides for,



LSIS RICHARD CORDELL, R.A. NAVY

Royal Australian Navy Collins Class Submarines joined in formation by United States Navy Los Angeles Class Submarine USS Santa Fe in the West Australian Exercise Area in 2019.

among other things, enhanced protections against the unauthorized disclosure of certain defense-related information. Australia's Defense Trade Controls Amendment Act 2024 and Safeguarding Australia's Military Secrets Act 2024 provide for controls on reexports of items originally exported from Australia, disclosures of controlled technology to certain foreign persons within Australia, and the provision of defense services.

These measures mitigate the risk of unauthorized use or diversion of those items subject to BIS's Export Administration Regulations, which may now be exported or reexported without a license to Australia and the UK. **With these changes, firearms-**

related items are the primary category of items that remain subject to a BIS license requirement to Australia and the UK.

Existing license requirements for the following items will remain in place:

- Certain satellites and related items
- Certain items controlled pursuant to the Chemical Weapons Convention, and items controlled for short supply reasons (e.g., certain petroleum products and Western red cedar)
- Certain law enforcement restraints and riot control equipment, implements of torture or execution, and horses exported by sea. [\[12073\]](#)

Commerce Concludes Firearms 'Pause'

The Department of Commerce released an interim final rule April 26 amending the Department's licensing policy for exports of firearms, ammunition, and related components under its jurisdiction. Coming on the six-month anniversary of a controversial "90 day pause" in firearms export license approval, the new rule proposes significant changes.

"Too often, firearms exports fall into the wrong hands and end up being used in ways that directly undermine U.S. national security and foreign policy interests," said **Commerce Secretary Gina Raimondo**, announcing the proposed rule. "To combat this, we're taking strategic, targeted actions, including restricting exports to commercial entities in high-risk countries and increasing scrutiny and tracking of all firearms exports,"

- The rule identifies semi-automatic firearms under new Export Control Classification Numbers (ECCNs);
- adds additional license requirements for Crime Control and Detection (CC) items, thereby resulting in additional restrictions on the availability of license exceptions for most destinations;
- amends license review policies so that they are more explicit as to the

nature of review that will accompany different types of transactions and license exception availability (including adding a new list of high-risk destinations);

- updates and expands requirements for support documentation submitted with license applications; and
- better accounts for the import documentation requirements of other countries (such as an import certificate or other permit prior to importation) when firearms and related items are authorized under a BIS license exception.

Industry Response

The National Shooting Sports Foundation (NSSF), representing American firearms manufacturers, objected to the proposed rules.

"This is deeply troubling the lengths to which this administration will go to turn the levers of government against a Constitutionally-protected industry in order to cozy up to special-interest gun control donors," said **Lawrence Keane**, NSSF Senior Vice President & General Counsel. "This is a wholesale attack on the industry that provides the means for Americans exercising their Second Amendment rights."

"The total economic impact of the

Interim Final Rule easily exceeds \$250 million to U.S. manufacturers and exporters, far above the farcically low estimates BIS has been telling NSSF and the Hill," Keane continued.

According to *The American Rifleman*, Turkey led the importing nations in 2020, with 1,478,464 firearms. Austria came in second at 1,284,785 followed by Brazil with 1,016,630. Rounding out the top five were Croatia (521,932) and Italy (360,557). None of the top export destinations were included in the list of restricted countries named in the proposed rule (see below).

More stringent review standards:

- BIS will increase scrutiny on a transaction-by-transaction level to help prevent firearms from ending up in the hands of foreign criminals, gangs, terrorists, or other malign actors. BIS is implementing regulations that list a clear set of national security and foreign policy factors to consider when reviewing a license application, including terrorism risks, human rights concerns, state fragility, corruption, the nature and capabilities of the firearm, and past instances of diversion and misuse.

Continues on next page

Continued from previous page

Presumption of denial for commercial transactions in countries the State Department has identified as high-risk:

- BIS will apply a “presumption of denial” standard to applications involving nongovernmental recipients located in a destination where the State Department has determined there is substantial risk that firearm exports will be diverted or misused in a manner contrary to national security and foreign policy.

- The State Department’s methodology and country list are included in its Firearms Guidance Memorandum. The Guidance Memorandum identifies 36 destinations where there is a substantial risk that firearms and related items exported to non-government end users will be diverted or misused in a manner adverse to U.S. national security and foreign policy.

- This is in addition to BIS’s policy of denial for countries subject to U.S. arms embargoes and for applications linked to drug trafficking, terrorism, and organized crime.

Data collection and transparency:

- BIS will improve data collection on firearms exports by adopting new



Private sales of firearms to countries like Kyrgyzstan, Laos, Mali and Yemen will be declined.

export control classification numbers (ECCNs) to track what kinds of firearms U.S. manufacturers are exporting abroad. These include **new ECCNs for semi-automatic firearms and related items.**

Additional documentation for license applicants:

BIS is implementing regulatory changes to licensing procedures that will help validate that firearms are only exported to trustworthy foreign entities.

- BIS is reducing the general license validity period from 4 years to 1 year, “which will ensure that BIS is able to adapt to an ever-changing global security environment.”

- Furthermore, for countries with less-developed export control regimes, BIS will require the submission of

additional documents from licensees before approving a license, including a purchase order and import certification.

Current Licenses Revoked

In addition to the new rule, on July 1, 2024, BIS will revoke currently valid licenses that authorize exports of firearms to non-government end users in the destinations identified by the State Department. This change will align future exports to the new IFR. Those licenses have not been reviewed under the updated policy, but license holders are welcome to reapply so that their applications can be reviewed under BIS’s new standard.

The IFR is effective on May 30, 2024, and the Department will accept public comments on the rule until July 1.

Less Export Promotion from ITA

In addition to the BIS IFR, Commerce’s International Trade Administration (ITA) is implementing changes to its Client Eligibility Policy that will curtail promotion of firearms exports and exports of other items destined for commercial end users that could be misused by malign actors. Any request falling into this category will be declined except in cases consistent with U.S. foreign policy objectives, including national security and human rights.

BRIEFS

FDP Rule Scope Expanded for Iran, Russia, Belarus

➤ Effective April 18th, the new rule from BIS amends the EAR to impose new controls restricting Iran’s access to additional low-level technology, including items manufactured outside the United States that are produced using U.S. technology. The rule also expands the scope of the Russia/Belarus/Temporarily occupied Crimea region of Ukraine Foreign Direct Product (FDP) rule. [\[12072\]](#)

Medical Device Exception to Russian Sanctions

➤ (BIS) published a final rule introducing the new License Exception MED, which authorizes certain exports, reexports, and transfers (in country) of low-level “medical devices” and related low-level “parts,” “components,” “accessories,” and “attachments” that are exclusively for use in or with “medical devices” to Russia, Belarus, the temporarily occupied Crimea region of Ukraine, and the covered regions of Ukraine. [\[12109\]](#)

State Dept. to Increase DDTC Fees

➤ For the first time in fifteen years, the State Department is proposing to revise and increase the registration fees for those required to register with the Directorate of Defense Trade Controls (DDTC). The Department has structured the registration fees into three tiers, based on the registrants’ interactions with DDTC and whether they have received any favorable determinations during a prescribed look-back period. [\[12091\]](#)

President Biden announces he has signed the \$95.3 billion foreign aid package at the White House in Washington, DC, on April 24.

C-SPAN VIDEO
FRAME



Aid Bill Includes Sanctions Lookback

Included among the munitions and TikTok drama, the foreign aid package signed April 24 has material changes for the sanctions compliance practitioner.

Incorporated in the final legislation is a bill from by **Sen. Sherrod Brown** (D-OH) and Sen Tim Scott (R-SC), [S. 1271], the FEND Off Fentanyl Act declaring fentanyl trafficking a national emergency and placing new sanctions on the leaders of trafficking organizations.

Front and center for sanctions practitioners is the extension of the statute of limitations for sanctions (SoL) violations from five to ten years. As the Sanctions team at Akin Gump notes in their review of the rule, “this change to the SoL will also apply to all other IEEPA-based legal authorities and programs, including certain national security programs administered and enforced by the U.S. Department of Commerce’s Bureau of Industry and Security (BIS), the U.S. Department of Justice’s National Security Division (DOJ-NSD) and the U.S. Department of the Treasury’s Office of Investment Security (Treasury OIS).

The final IEEPA SoL is in Section 3111 of the new law, [PL 118-50] which amends 50 U.S.C. Section 1705(d) to say:

“An action, suit, or proceeding for the enforcement of any civil fine, penalty, or forfeiture, pecuniary or otherwise, under this section shall not be entertained unless commenced within 10 years after the latest date of the violation upon which the civil fine, penalty, or forfeiture is based.”

Tim O’Toole of Miller & Chevalier, points out to the Wall Street Journal, “When companies discover a possible sanctions violation, they often do a five-year lookback to see if it was a one-off or whether the problem is a systemic one. Companies may now have to do a 10-year lookback, including for companies they are looking to acquire.”

Anti Money Laundering

The measure gives the U.S. Treasury Department more latitude to combat money laundering

Continues on next page

Continued from previous page

tied to trafficking and gives officials the authority to make use of forfeited property for law enforcement efforts. If the Secretary of the Treasury determines that reasonable grounds exist for concluding that

- One or more financial institutions operating outside of the United States,
- One or more classes of transactions within, or involving, a jurisdiction outside of the United States, or

• One or more types of accounts within, or involving, a jurisdiction outside of the United States, is of primary money laundering concern in connection with illicit opioid trafficking, the Secretary of the Treasury may, by order, regulation, or otherwise as permitted by law —

- require domestic financial institutions and domestic financial agencies to take 1 or more of the special measures provided for in section

9714(a)(1) of the National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283; 31 U.S.C. 5318A note); or

- prohibit, or impose conditions upon, certain transmittals of funds (to be defined by the Secretary) by any domestic financial institution or domestic financial agency, if such transmittal of funds involves any such institution, class of transaction, or type of accounts. [\[12118\]](#)

May Day Russian Sanctions Target 300

May 1st the Treasury Department issued sanctions targeting Russia’s military-industrial base and chemical and biological weapons programs, as well as companies and individuals in third countries that help Russia acquire key inputs for weapons or defense-related production.

“Treasury has consistently warned that companies will face significant consequences for providing material support for Russia’s war, and the U.S. is imposing them today on almost 300 targets,” said **Secretary of the Treasury Janet L. Yellen**.

The action includes nearly 60 targets located in Azerbaijan, Belgium, the PRC, Russia, Slovakia, Türkiye, and the United Arab Emirates (UAE). Among the entities named are Chinese and Russian firms responsible for the manufacture and sale of nitrocellulose, a key ingredient in high explosives.

State Targets Chem-Bio Warfare

In addition to the nearly 200 targets sanctioned by the Treasury Department [list], the Department of State is imposing sanctions on over 80 entities and individuals that are engaged in sanctions evasion and circumvention or are related to Russia’s chemical and biological weapons programs and defense industrial base.

State is concurrently delivering to Congress a determination pursuant to the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991 (CBW Act) regarding Russia’s use of the chemical weapon chloropicrin against Ukrainian troops. Pursuant to the CBW Act, the Department

is re-imposing restrictions on foreign military financing, U.S. Government lines of credit, and export licenses for defense articles and national security-sensitive items going to Russia.

The Department also is sanctioning three Russian government entities associated with Russia’s chemical and biological weapons programs and four Russian companies that have contributed to such entities. Among these actions, the Department is also sanctioning an additional three individuals in connection with the death of **Aleksey Navalny** in Russian Penal Colony IK-3.

Energy Infrastructure Targeted

The Department is designating two vessel operators involved in the transport of highly specialized liquefied natural gas (LNG) modules and gravity-based structure (GBS) equipment designed specifically for Russia’s Arctic LNG 2 project, as well as Hong Kong, Singapore and Russian companies providing maritime logistics and construction support for Russian energy projects, including Arctic LNG 2.

As well, State is designating 12 entities within the **Sibanthracite** group of companies, one of Russia’s largest producers of metallurgical coal, and State Atomic Energy Corporation Rosatom (**Rosatom**) subsidiaries distributing machine tools for the enterprise.

Russian Nuclear Largely Untouched

Rosatom, which produces 43% of the world’s

enriched uranium, continues to profit handsomely off of commerce with the West. Europe has 19 Russian-designed reactors in five countries that are fully dependent on Russian nuclear fuel, according to reporting by VOA. The U.S. Senate approved on legislation to bar imports of Russian uranium. U.S. nuclear power plants imported around 12% of their uranium from Russia in 2022, according to the U.S. Energy Information Administration.

Aircraft Parts Forfeiture Filed

In a related action, The Justice Department filed a forfeiture complaint against a set of aircraft landing gear for a Boeing 737-800 that was detained in September 2023 at Miami International Airport by U.S. Customs and Border Patrol.

The gear was purchased for \$1.55 million for the benefit of a Kyrgyz Republic-based transhipper of dual-use items servicing the Russian Federation, in violation of U.S. sanctions on LLC RM Design and Development, which was designated by OFAC in July 2022. [\[12136\]](#)



ADOBESTOCK

The U.S. Senate approved on legislation to bar imports of Russian uranium. U.S. nuclear power plants imported around 12% of their uranium from Russia in 2022.

BRIEFS

EU-wide Minimum Rules for Sanctions Prosecution

► the Council of the European Union adopted a law covering EU-wide minimum rules for the prosecution of violation or circumvention of EU sanctions in member states. Certain actions will now be considered criminal offences in all member states, for example helping to bypass a travel ban, trading in sanctioned goods or performing prohibited financial activities. Inciting, aiding and abetting these offences can also be penalized. [\[12042\]](#)

U.S. & UK Institute Joint Metals Trading Ban

► In a joint action with UK officials, the Treasury Department issued two new prohibitions to disrupt the revenue that Russia earns from its export of aluminum, copper, and nickel. This new action prohibits the import of Russian-origin aluminum,

copper, and nickel into the U.S. and UK, and limits the use of Russian-origin aluminum, copper, and nickel on global metal exchanges and in over-the-counter derivatives trading. [\[12048\]](#)

Treasury Seeks New Sanctions Tools

► Treasury Deputy Secretary Wally Adeyemo told the Senate Banking Committee that the Administration needs “additional tools to protect the American people” suggesting Congress strengthen counter-terrorist financing authorities. Proposals include new secondary sanctions tools, expansion of authorities into the digital realm, and jurisdictional fixes related to cryptocurrency. [\[12052\]](#)

China Sanctions more U.S. Defense Firms

► Dronemaker General Atomics Aeronautical Systems and General



GENERAL ATOMICS

MQ-9B SeaGuardian. Dronemaker General Atomics Aeronautical Systems and General Dynamics Land Systems, have been sanctioned by the Chinese government for their sales to the government of Taiwan.

Dynamics Land Systems, have been sanctioned by the Chinese government for their sales to the government of Taiwan. Last September China sanctioned Northrop Grumman and Lockheed Martin on the same grounds. Missing from either announcement was Boeing, Taipei’s supplier of Harpoon anti-ship missiles. [\[12041\]](#)

Continues on next page

Chinese and Belarus Ballistic Missile Suppliers

➤ The State Department designated four entities pursuant to Executive Order 13382, which targets proliferators of weapons of mass destruction and their means of delivery. The entities – three based in the People’s Republic of China and one in Belarus — have supplied missile-applicable items to Pakistan’s ballistic missile programs, including its long-range missile program. [\[12074\]](#)

Belarus Sanctions Broadened

➤ In an effort to further isolate the Russian and Belarus military-industrial complex, Treasury’s Office of Foreign Assets Control (OFAC) is designating six revenue-generating state-owned enterprises (SOEs) and one entity and five individuals involved in facilitating transactions for a U.S.-designated major Belarusian defense sector enterprise. [\[12069\]](#)



STANKOGOMEL

5-axis vertical machining center by OJSC StankoGomel

Iran UAV Suppliers

➤ OFAC is sanctioning over one dozen entities, individuals, and vessels that have played a central role in facilitating and financing the clandestine sale of Iranian unmanned aerial vehicles (UAVs) for Iran’s Ministry of Defense and Armed Forces Logistics (MODAFL),

which itself is involved in supporting Iran’s Islamic Revolutionary Guard Corps (IRGC) and Russia’s war in Ukraine. [\[12112\]](#)

Iran Facilitators & Vessels

➤ OFAC announced it is targeting a network facilitating shipments valued in the hundreds of millions for the Iranian military, as well as identifying 13 vessels managed by Oceanlink Maritime DMCC as blocked property. [\[12015\]](#)

Entity List: UAE, Russian, Chinese Traders

➤ Commerce Department’s Bureau of Industry and Security (BIS) added 11 entities to the Entity List. Five of the eleven entities are Russian and PRC entities were added for actions related to unmanned aerial vehicles (UAVs). Of these, four are part of a procurement network for components for UAV applications. [\[12027\]](#)

More Iran UAV Suppliers & Steelmaker

➤ OFAC targeted 16 individuals and two entities enabling Iran’s UAV production, including engine types that power Iran’s Shahed variant UAVs, which were used in the April 13 attack on Israel. Also designated are five companies in multiple jurisdictions providing component materials for steel production to Iran’s Khuzestan Steel Company (KSC), or purchasing KSC’s finished steel products. [\[12065\]](#)

Russian Airline TDO Extended

➤ BIS extended the Temporary Denial Order for Russian air cargo operator Aviastar-TU initially imposed in April 2022. Aviastar continued to operate Boeing aircraft subject to the EAR, including, but not limited to, on flights into and out of Russia from/to Hangzhou, China as well as domestically within Russia [\[12006\]](#)



Bahman Trail 230 Motorcycle. OFAC is also sanctioning three subsidiaries of Iranian automaker Bahman Group.

Iran Cyber Actors, Tuareg Kidnappers

➤ OFAC announced sanctions on Iranian cyber responsible for more than a dozen U.S. companies and government entities through cyber operations, including spear phishing and malware attacks. OFAC has also sanctioned two leaders of al-Qa’ida-aligned terrorist group Jama’at Nusrat al-Islam wal-Muslimin (JNIM) for hostage-taking of U.S. persons in West Africa. [\[12099\]](#)

DPRK in Thailand; Iraq - Sudan Arms Trade

➤ Two men were charged with conspiring to export munitions from the United States to Sudan and Iraq without the necessary licenses and approvals, in violation of the Arms Export Control Act. As well, an indictment was unsealed charging a former North Korean official serving in Thailand with conspiracy to violate U.S. economic sanctions bank fraud, and international money laundering. [\[12061\]](#)

Hamas Cyber & UAV Officials

➤ OFAC is taking action against Hamas, targeting Gaza- and Lebanon-based leaders of the terrorist group’s offensive cyber and unmanned aerial vehicle (UAV) operations. Concurrent with this action, the European Union is imposing sanctions targeting Hamas. [\[12043\]](#)

PCAOB

Auditor Cheating Reflects ‘inappropriate tone at the top’

Public Company Accounting Oversight Board (PCAOB) Chair **Erica Y. Williams** announced a record \$25 million fine sanctioning KPMG Netherlands for widespread improper answer sharing and the firm’s multiple misrepresentations about its knowledge of the misconduct.

“The widespread exam cheating went on for a period of five years, from 2017 to 2022, and involved hundreds of professionals, reaching as far as partners and senior firm leaders — including the firm’s former Head of Assurance, who is also facing a \$150,000 penalty and permanent bar under today’s orders.

“The growth and breadth of exam cheating in this case was enabled by the firm’s failure to take appropriate steps to monitor, investigate, and identify the potential misconduct.

“Furthermore, during the course of our investigation, the firm submitted — and failed to correct — multiple inaccurate representations to the PCAOB.

“For example, the firm claimed to have no knowledge of answer sharing prior to a 2022 whistleblower report. Yet, this could not have been true because members of the firm’s Management Board and Supervisory Board who signed off on that submission to the PCAOB had, in fact, cheated themselves.

“**But it doesn’t end there.** KPMG Netherlands’ CEO learned the submissions were inaccurate and failed to inform anyone until months later, when a second whistleblower came forward.

Only then did the firm correct the inaccurate representations to investigators.

“This misconduct reveals an inappropriate tone at the top and a complete failure by firm leadership to promote an ethical culture worthy of investors’ trust.”

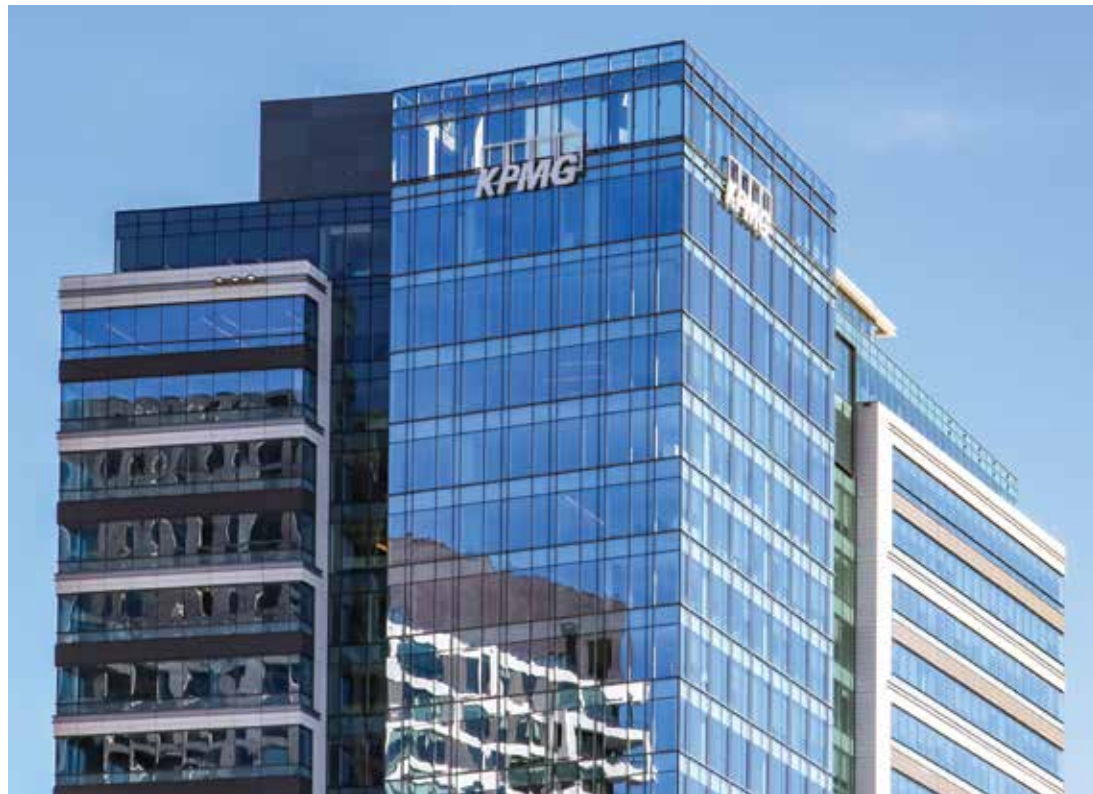
CAOB also announced \$2 million in fines against Deloitte Indonesia and Deloitte Philippines for violations of PCAOB rules and quality control deficiencies that resulted in widespread answer sharing on internal training tests.

The PCAOB has imposed \$34 million in penalties this year alone. Since 2021, the PCAOB has sanctioned nine registered firms for exam cheating, including PwC China and PwC Hong Kong in November, 2023. [\[11455\]](#)

The largest source of funding for the PCAOB’s \$385 million budget comes from the companies whose financial statements must be audited by PCAOB-registered firms. [\[12030\]](#)

PCAOB Chair Erica Y. Williams announced a record \$25 million fine sanctioning KPMG Netherlands.

ADOBESTOCK/
JHVEPHOTO

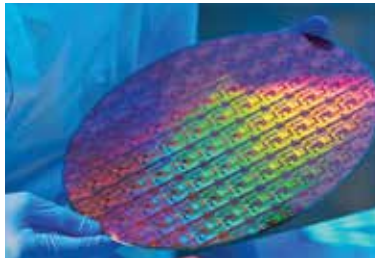


Chinese Nabbed in Chip Equipment Ruse

Two Chinese nationals were charged with crimes related to a conspiracy to illegally export U.S. technology to prohibited end users in China, in violation of the International Emergency Economic Powers Act (IEEPA) and Export Administration Regulations (EAR). Lin Chen was arrested in Chicago April 25, Han Li remains at large. The two are charged with attempting to procure a machine manufactured by a California-based company that is used to process silicon wafer microchips.

“The export restrictions at issue in this case were put in place to prevent the illicit procurement of commodities and technologies for unauthorized military end use in the People’s Republic of China,” said **U.S. Attorney Ismail Ramsey** for the Northern District of California.

In August 2014, the Commerce Department added Changdu GaStone Technology Company (CGTC), a company based in China, to the Entity List. Between at least May 2015 and August 2018, Li and Chen conspired to evade the export restrictions imposed by the Department of Commerce on CGTC through the use of intermediaries to conceal CGTC’s involvement with the transactions.



ADOBESTOCKRYANKING999

The two are charged with attempting to procure a machine used to process silicon wafer microchips.

Specifically, the defendants sought to illegally obtain a DTX-150 Automatic Diamond Scriber Breaker machine from Dynatex International, a Santa Rosa, California, company. The machine is used to cut thin

semiconductors used in electronics, also known as silicon wafers, and under Department of Commerce regulations, requires a license and authorization to export to CGTC.

The defendants sought to acquire the machine for CGTC through an intermediary company called Jiangsu Hantang International (JHI), a proxy they fraudulently represented as the purchaser and end user. To avoid detection, Li and Chen instructed Dynatex Inter-

national to ensure that the export information associated with the sale did not list CGTC as the ultimate consignee of the shipment.

Li and Chen each are charged with the following offenses, and if convicted, face maximum penalties as indicated: Conspiracy to violate IEEPA, up to 20 years in prison and a \$1 million fine; false electronic export information activities, up to five years in prison and a \$250,000 fine; smuggling, up to 10 years in prison and a \$250,000 fine; and IEEPA violations, up to 20 years in prison and a \$1 million fine. [\[12116\]](#)

OFAC

Thai Plastics Firm Fined \$20 Million for Iran Sanctions

Treasury’s Office of Foreign Assets Control (OFAC) Friday announced a settlement with SCG Plastics Co., Ltd., part of a multinational enterprise headquartered in Bangkok, Thailand. SCG Plastics has agreed to pay \$20,000,000 to settle its potential civil liability for 467 apparent violations of OFAC sanctions on Iran.

From 2017 to 2018, SCG Plastics caused U.S. financial institutions to process \$291 million in wire transfers for sales of Iranian origin polyethylene

resin manufactured by a joint venture in Iran. In 2005 SCG entered into a joint venture to construct and operate a petrochemical plant in Iran, with SCG to offtake 60 percent of production. SCG repeatedly issued shipping and payment documents that replaced the word “Iran” with variants of the term “Middle East.” Pro-forma invoices listed the loading port as “any port in the Middle East.” Transshipment through the UAE enabled the firm to claim

Jebel Ali, UAE as Port of Origin.

In July 2018, after the United States announced it was withdrawing from the Joint Comprehensive Plan of Action, SCG sold its interest in the plant and ended its sales of Iranian-origin HDPE.

The \$20,000,000 settlement amount reflects OFAC’s determination that SCG Plastics’ apparent violations were egregious and, with the exception of certain transactions, were not voluntarily self-disclosed.



US TREASURY DEPT

Dassault Falcon 900ex registered to PDVSA, the Venezuelan state-owned oil company sanctioned by the U.S.

Arrest in Executive Jet Fleet Scheme for Venezuelans

The Justice Department announced the unsealing of an indictment charging 10 defendants with conspiring to violate the International Economic Emergency Powers Act (IEEPA) for their roles in a scheme to evade U.S. sanctions imposed on Petróleos de Venezuela, S.A. (PDVSA), the Venezuelan state-owned oil company. One of the defendants, George Clemente Semerene Quintero, 60, was arrested on April 19, upon arrival at the Miami International Airport.

Between January 2019 and December 2021, after learning of the sanctions imposed on PDVSA, the defendants devised a scheme to illegally procure aircraft parts, including Honeywell Turbofan Engines, from the United States to service PDVSA's aircraft fleet in Venezuela, in violation of U.S. sanctions and export controls.

PDVSA maintains a fleet of business aircraft, including

- 5 Dassault Falcon Jets
- 7 Bombardier Learjet 45s
- 3 Beech 1900D

To carry out this scheme, the defendants concealed from U.S. companies that the goods were destined for Venezuela and PDVSA by exporting them to third parties in other countries, including Novax Group SA (Novax), a Costa Rican company, and Aerofalcon SL (Aerofalco), a Spanish com-

pany. The Department of Commerce added Novax and Aerofalcon to its Entity List in November 2023.

According to court documents, the defendants include:

- Four individuals associated with PDVSA: a PDVSA air transport manager and colonel in the Venezuelan military; two PDVSA air transport managers and logistics analysts responsible for procurement; and PDVSA's head of logistics, procurement and warehousing.
- Four individuals associated with Novax and two individuals associated with Aerofalcon.

The defendants are charged with conspiring to violate IEEPA, and if convicted, face a maximum penalty of 20 years in prison. Four defendants are additionally charged with submitting false or misleading export information and smuggling of goods, which respectively carry maximum penalties of five and 10 years in prison.

Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division, Assistant Secretary for Export Enforcement Matthew S. Axelrod of the Commerce Department's Bureau of Industry and Security (BIS), and U.S. Attorney Markenzy Lapointe for the Southern District of Florida made the announcement. BIS continues investigating the case. [\[12097\]](#)

Miami-Based Russians Guilty in Aircraft Parts Scheme

Two Russian nationals pleaded guilty last week to conspiracy to violate the Export Control Reform Act (ECRA) in connection with a scheme to acquire and unlawfully export controlled aviation technology to Russian end users. One of the defendants, Oleg Patsulya, also pleaded guilty to conspiracy to commit international money laundering.

According to court documents, Patsulya and Vasilii Besedin, both of whom reside in Miami-Dade County, Florida, conspired with each other and several others to evade U.S. export laws and regulations to send aircraft technology from the United States to Russia.

According to court documents, the unlawful scheme began in or about May 2022, in the wake of Russia's most recent invasion of Ukraine and enhanced U.S. sanctions on Russia.

"Disrupting the illegal export of sensitive American goods and technologies to sanctioned foreign actors is a critical priority requiring a whole-of-government approach," said **U.S. Attorney Gary Restaino** for the District of Arizona. "This case has been a textbook example of how a collaborative strike force can work together effectively and nimbly to dismantle a sanctions-evad-

ing scheme and to prosecute those individuals who profit from it."

Beginning in or about May 2022 through on or about May 11, 2023, Patsulya and Besedin conspired with each other and several others to obtain orders for various aircraft parts and components from Russian buyers — primarily commercial airline companies — and then fulfill those requests by acquiring the parts from the United States suppliers, including a supplier based in Arizona, and unlawfully exporting the parts to Russia. The defendants admitted to knowing the items were controlled and required a license from the Department of Commerce to export.

For example, the defendants conspired to export multiple shipments of a carbon disc brake system used on Boeing 737 aircraft. When they contacted various U.S. suppliers in efforts to obtain the brake system, Besedin and Patsulya provided false information that the parts were intended for countries other than Russia. The United States was able to detain, prior to export, multiple shipments made by the defendants containing units of the brake assembly technology.

Besedin and Patsulya further admitted that they

Aeroflot Boeing 737-8MC.

ANNA ZVEREVA/
CC BY-SA 2.0



attempted to conceal the illegal exports and avoid detection by law enforcement, including by making false representations about the identities of their true customers and using straw buyer-companies located overseas to obscure the origin of revenue. For example, on Sept. 8, 2022, Besedin and Patsulya traveled to Arizona to close a deal with a U.S. company, in which the defendants sought to purchase units of the brake assembly technology.

During their discussions with the company, the defendants misrepresented that the aircraft parts were going to be exported to Turkey, when they were in fact destined for Russia. The defendants made false statements both orally to the company and in the export compliance forms. In connection with this transaction, the defendants received money from a Russian airline company to make the purchase. The funds were transferred to Patsulya's American bank account from a Turkish bank ac-

count which had previously received the money from Russia.

In total, throughout the conspiracy, American bank accounts associated with MIC P&I LLC, a company controlled by Patsulya, received at least \$4,582,288 sent from Russian airline companies through Turkish bank accounts to purchase aircraft parts and components intended for unlawful export. As part of Patsulya's plea, he agreed to forfeit, among other assets, a sum of money equal to \$4,582,288.

Both Besedin and Patsulya pleaded guilty to conspiracy to export items from the United States without a license in violation of the Export Control Reform Act, which carries a maximum penalty of 20 years in prison. Patsulya additionally pleaded guilty to one count of conspiracy to commit international money laundering, which carries a maximum penalty of 20 years in prison. [\[12020\]](#)

Steel Trader Sentenced to Six Years, \$160 million Forfeiture

The president of Orlando, Florida-based steel trading firm Metalhouse LLC, was sentenced to six years in prison for conspiracy to commit money laundering to promote violations of U.S. sanctions against Sergey Kurchenko, a pro-Russian Ukrainian oligarch. A business associate, a Belarusian national residing in Miami, was sentenced to 21 months in prison for his role in the scheme.

John Unsalan pleaded guilty and was ordered

to forfeit \$160 million in proceeds from the offense. Karpushkin pleaded guilty to conspiring to violate the International Emergency Economic Powers Act (IEEPA) and to commit international promotional money laundering and was ordered to forfeit \$4.7 million in criminal proceeds.

Kurchenko was sanctioned by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) in 2015 for his role in misappropriating state assets of Ukraine or of an eco-



nomically significant entity in Ukraine. Two sanctioned companies — Kompaniya Gaz-Alyans OOO, based in the Russian Federation and controlled by Kurchenko, and ZAO Vneshtorgservis, based in the Russian occupied Georgian region of South Ossetia – were designated by OFAC in 2018 for acting on behalf of and providing material support to the so-called Donetsk People's Republic and Luhansk People's Republic in the separatist-controlled regions of eastern Ukraine.

As set forth in court filings, Unsalan and Sergey Karpushkin engaged in trade with these sanctioned individuals and entities to procure steelmaking equipment and raw material despite knowing that Kurchenko, Gaz-Alyans and Vneshtorgservis were subject to U.S. sanctions that prohibited U.S. persons and entities from doing business with them.

No licenses from OFAC were applied for or issued for these payments or

transfers.

As stated in court documents, between July 2018 and October 2021, Unsalan conspired with others to transfer over \$150 million to Kurchenko and companies controlled by Kurchenko. Unsalan, acting through his company, Metalhouse, engaged in trade with sanctioned individuals and entities and received tens of thousands of tons of metal products from the companies.

Between July 2017 and August 2020, Karpushkin conspired with Unsalan and other business associates, acting through Metalhouse, to enter into contracts and purchase orders for pig iron, steel billets, and wire rods from these sanctioned companies and agreed to share profits from these unlawful transactions.

The co-conspirators intentionally concealed from U.S. banks and government officials the ultimate source and origin of the goods that they sought to acquire, knowing that they did not have the necessary authorization or license from OFAC to transact with Kurchenko and companies owned and controlled by Kurchenko. [\[11211\]](#)

Ecuador Official Convicted in Odebrecht Bribery Case

A federal jury in Miami has convicted the former Comptroller General of Ecuador for his role in a multimillion-dollar international bribery and money laundering scheme.

According to court documents and evidence presented at trial, between 2010 to 2015, Carlos Ramon Polit Fagioni, 73, solicited and received over \$10 million in bribe payments from Odebrecht S.A., the Brazil-based construction conglomerate.

Polit took bribes from Odebrecht in exchange for removing fines and not imposing fines on Odebrecht's projects in Ecuador. Additionally, in or around 2015, Polit received a bribe from an Ecuadorian businessman in exchange for assisting the businessman with obtaining certain contracts with the state-

owned insurance company of Ecuador.

"This verdict is a reminder of our office's firm commitment to investigating and prosecuting corrupt foreign officials who bring their criminally obtained funds to South Florida to buy real estate," said **U.S. Attorney Markenzy Lapointe for the Southern District of Florida**.

From in or around 2010 and continuing until at least 2017, at the direction of Polit, another member of the conspiracy caused proceeds of Polit's bribery scheme to "disappear" by using Florida companies registered in the names of friends and associates, often without the associates' knowledge. The conspirators also used funds from Polit's bribery scheme to purchase and renovate real estate in Florida.

The jury convicted Polit of one count

of conspiracy to commit money laundering, three counts of concealment money laundering, and two counts of engaging in transactions in criminally derived property. He faces a maximum penalty of 20 years in prison on each count of money laundering and conspiracy to commit money laundering and a maximum penalty of 10 years in prison on each count of engaging in transactions in criminally derived property.

Odebrecht S.A. pleaded guilty in December 2016 in the Eastern District of New York to conspiring to violate the anti-bribery provisions of the Foreign Corrupt Practices Act (FCPA) in connection with a broader scheme to pay nearly \$800 million in bribes to public officials in 12 countries, including Ecuador. [\[12107\]](#)

Handbag Maker Sentenced for CITES Violations

Luxury handbag company Gzuniga Ltd., its founder Nancy Teresa Gonzalez de Barberi and an associate were sentenced to prison for illegally importing merchandise from Colombia to the United States that was made from protected wildlife. All had previously pleaded guilty.

Gzuniga was ordered to forfeit all handbags and other previously seized product, banned for three years from any activities involving commercial trade in wildlife and sentenced to serve three years of probation. Gonzalez was sentenced to 18 months in prison with credit for time served, a supervised release of three years and to pay a special assessment.

An indictment charged Gzuniga, Gonzalez, and associates with one count of conspiracy and two counts of smuggling for illegally

importing designer handbags made from caiman and python skin from February 2016 to April 2019. The caiman and python species are protected by

the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES), to which both the United States and Colombia are signatories.

The conspirators brought hundreds of designer purses, handbags and totes into the United States by enlisting friends, relatives and even employees of Gonzalez's manufacturing company in Colombia to wear the designer handbags or put them in their luggage while traveling on passenger airlines. Once in the United States, the bags were delivered or shipped to the Gzuniga showroom New York to be displayed and sold. [\[12095\]](#)



JUSTICE DEPARTMENT PHOTO

‘Toothless’ EU Forced Labor Legislation Passed

The European Parliament has given its final approval to a new regulation enabling the EU to prohibit the sale, import, and export of goods made using forced labor.

Member state authorities and the European Commission will be able to investigate suspicious goods, supply chains, and manufacturers. If a product is deemed to have been made using forced labor, it will no longer be possible to sell it on the EU market (including online) and shipments will be intercepted at the EU’s borders.

Originally proposed in 2021, the rulemaking had been stymied by resistance from industry groups, with the final result lacking much of the efficacy of the U.S. version, the Uyghur Forced Labor Protection Act.

Loopholes include a provision allowing national authorities to ask companies that provide “critical products” to withhold their products until they can demonstrate no more links to forced labor in their operations, essentially delaying the bans.

More meaningfully, there is no presumption of state-imposed forced labor in high-risk areas and sectors where there is evidence of slave labor.

“The Commission proposes to exclude goods from the market only after the existence of forced labor in their supply chain has been established, not when it is suspected,” a German MP objected.

In U.S. legislation, authorities may prohibit imports based on reasonable suspicion. The U.S. framework also places the onus on companies to prove their products are free from forced labor.

The EU proposal, in contrast, places the burden of proof on European authorities, which are under-resourced and would end up doing piecemeal enforcement, critics say.

Instead of presumptions or regional bans, the EU Commission will have to draw up a list of those areas and sectors and an online platform will be set up “for stakeholders to check all available information.”

Investigations

Decisions to investigate “will be based on factual and verifiable information that can be received from, for example, international organizations, cooperating authorities and whistle-blowers,” according to the European Parliament.

Several risk factors and criteria will be taken into account, including the prevalence of state-imposed forced labor in certain economic sectors and geographic areas.

Consequences for companies using forced labor

Once the process of evaluation is complete, manufacturers of banned goods will have to withdraw their products from the EU single market and donate, recycle or destroy them.

Non-compliant companies could be fined. The goods may be allowed back on the EU single market once the company eliminates forced labor from its supply chains.

Earlier last month, **Chairman Mike Gallagher** (R-WI) and **Ranking Member Raja Krishnamoorthi** (D-IL) of the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party wrote to **Secretary of State Antony Blinken**, urging the State Department to increase diplomacy to ensure companies profiting off the CCP’s ongoing genocide in Xinjiang are not able to access global markets.

In the letter, the lawmakers write, “We are particularly concerned that goods made by Uyghur forced labor continue to flood into Europe and the United Kingdom (UK), which some have described as ‘dumping grounds’ for these products that are otherwise banned from importation into the United States.

The State Department plays a critical role in working with our allies and partners to ensure that companies profiting off the CCP’s ongoing genocide in Xinjiang find no safe markets for their wares.” [\[12110\]](#)

To read complete articles, click on the [Story ID number](#).

Customs / HSI Up Textile Enforcement Efforts

The Department of Homeland Security (DHS) is launching an enhanced strategy to combat illicit trade and support the American textile industry, with collaborative efforts between U.S. Customs and Border Protection (CBP) and Homeland Security Investigations (HSI).

The enforcement plan includes targeting small package shipments to prevent the entry of illicit goods, conducting joint CBP-HSI operations for cargo compliance, expanding audits and foreign verifications, and broadening the Uyghur Forced Labor Prevention Act (UFLPA) Entity List.

Key actions are improving package screening for textile violations, conducting physical inspections and testing for cargo compliance, assessing risks through customs audits, increasing education for stakeholders, and leveraging industry partnerships to facilitate legitimate trade.

The new enforcement plan focuses on the following actions:

- **Cracking down on small package shipments to prohibit illicit goods from U.S. markets** by improving screening of packages claiming the Section 321 de minimis exemption for textile, UFLPA, and other violations, including ex-

panded targeting, laboratory and isotopic testing, and focused enforcement operations.

- **Conducting joint CBP-HSI Trade special operations to ensure cargo compliance.** This includes physical inspections; country-of-origin, isotopic, and composition testing; and in-depth reviews of documentation. CBP will issue civil penalties for violations of U.S. laws and coordinate with HSI to develop and conduct criminal investigations when warranted.

- **Better assessing risk by expanding customs audits and increasing foreign verifications.** DHS personnel will conduct comprehensive audits and textile production verification team visits to high-risk foreign facilities to ensure that textiles qualify under the U.S.-Mexico-Canada Agreement (USMCA) or the Central America-Dominican Republic Free Trade Agreement (CAFTA-DR). CBP recently visited 31 facilities in Mexico — the first such visits under USMCA — as well as 18 facilities in Honduras, and is on track to double the number of total foreign verification visits compared to last year.

- **Building stakeholder awareness** by engaging in an education campaign to ensure that importers and suppliers in the CAFTA-DR and USMCA region

understand compliance requirements and are aware of CBP's enforcement efforts.

- **Leveraging U.S. and Central American industry partnerships** to improve facilitation for legitimate trade.

- **Expanding the UFLPA Entity List** to identify malign suppliers for the trade community through review of additional entities in the high-priority textile sector for inclusion in the UFLPA Entity List.

Following a January meeting with members of the National Council of Textile Organizations (NCTO) to discuss current challenges in the textile industry, Secretary Mayorkas directed the Department to provide him with a new comprehensive enforcement action plan to increase and expedite their work to combat illegal customs practices that harm the American textile industry.

"DHS is committed to expanding the UFLPA Entity List and sending a strong message to the importing community that the United States has zero tolerance for forced labor in our supply chains," said Robert Silvers, Under Secretary for Policy and Chair of the Forced Labor Enforcement Task Force. "Enforcing our forced labor laws protects human rights and businesses and workers who play by the rules and should not be undercut by predatory and abusive labor practice." [12005]



Intangible Transfers of Technology and Software

SIPRI Report Examines NewSpace Cases

Controlling intangible transfers of technology (ITT) and software — including in the context of the Missile Technology Control Regime (MTCR) — is a known challenge, but the growth of the NewSpace industry and advances in emerging technologies make it a particularly timely topic.

This report from SIPRI explores a series of cases

of export control violations and cases where the risk of a possible violation was identified involving missile-related ITT or software. The report also develops a typology of violations and identifies associated compliance challenges.

Key challenges emerge from the typology and the analysis of case studies. The increasing reliance on ITT and software by companies in the aerospace

and NewSpace sectors and their global supply chains presents one such challenge. Digital transfers of technology and software, including through cloud-based servers, have also become easier and as a result more common. Despite this, many companies, especially recently established NewSpace and emerging technologies start-ups, lack detailed awareness of ITT and software controls or effective methods of ensuring compliance with such controls.

Compliance is also a challenge among research institutes and especially in academia, where research is being undertaken in fields that are highly relevant to missile development. Actors actively seeking to acquire technology and software to advance their missile programs can take advantage of this. They could also exploit the increasing trend for foreign direct investment (FDI) to access technology by gaining control of or ownership rights over a company.

The report concludes by offering recommendations for the MTCR to strengthen its efforts to address the proliferation risks posed by ITT and software. [\[12169\]](#)

SpaceX's Starship rocket prototypes are seen at the SpaceX Starbase in Brownsville, Texas

SPACEX



USMCA BRIEFS

Mexico Wins First USMCA RRLM Case

► The first arbitration panel under the U.S.-Mexico-Canada rapid response labor mechanism has ruled in favor of Mexico in the case of the San Martín mine, located in Sombrerete, Zacatecas.

The three members of the panel determined that they did not have jurisdiction to rule on the denial of union rights at the mine, because the problems occurred before the USMCA took effect, according to a release from Mexico's Ministry of Economy. [\[12140\]](#)

Call Center Determination Appealed

► The U.S. TR has requested a Rapid Response Labor Mechanism (RRM) panel

under the United States-Mexico-Canada Agreement (USMCA) to resolve a labor dispute at call center operator Atento Servicios, S.A. de C.V. At the conclusion of its 45-day review period, Mexico found a denial of rights had existed, but determined that Atento Servicios had taken the necessary actions to remediate the denial of rights during Mexico's review period. The United States disagrees with this determination and is requesting establishment of an RRM panel to review the situation. [\[12058\]](#)

Japan - Mexico JV Targeted

► The U.S. has filed a complaint that workers at a Joint venture of of Industrias Peñoles, Japan's Sumitomo Corp. and Dowa Metals & Mining are being denied the right to freedom of association and collective bargaining. The zinc concen-

trates produced at Tizapa are sent to Japan for processing, i.e. there is no U.S. nexus. As Asian firms develop their Mexican manufacturing to address Latin American markets, such disputes may be expected to increase. [\[12002\]](#)

Automotive Supplier Suits Settled

► The United States announced two resolutions of labor disputes initiated under the USMCA facility-specific Rapid Response Labor Mechanism (RRM) in Mexico last year. The Turkish owners of the Teklas Automotive hose assembly plant and the Mexican owners of the Draxton automotive casting operations, both in central Mexico, conducted remediation satisfactory to U.S. officials. [\[12023\]](#)

