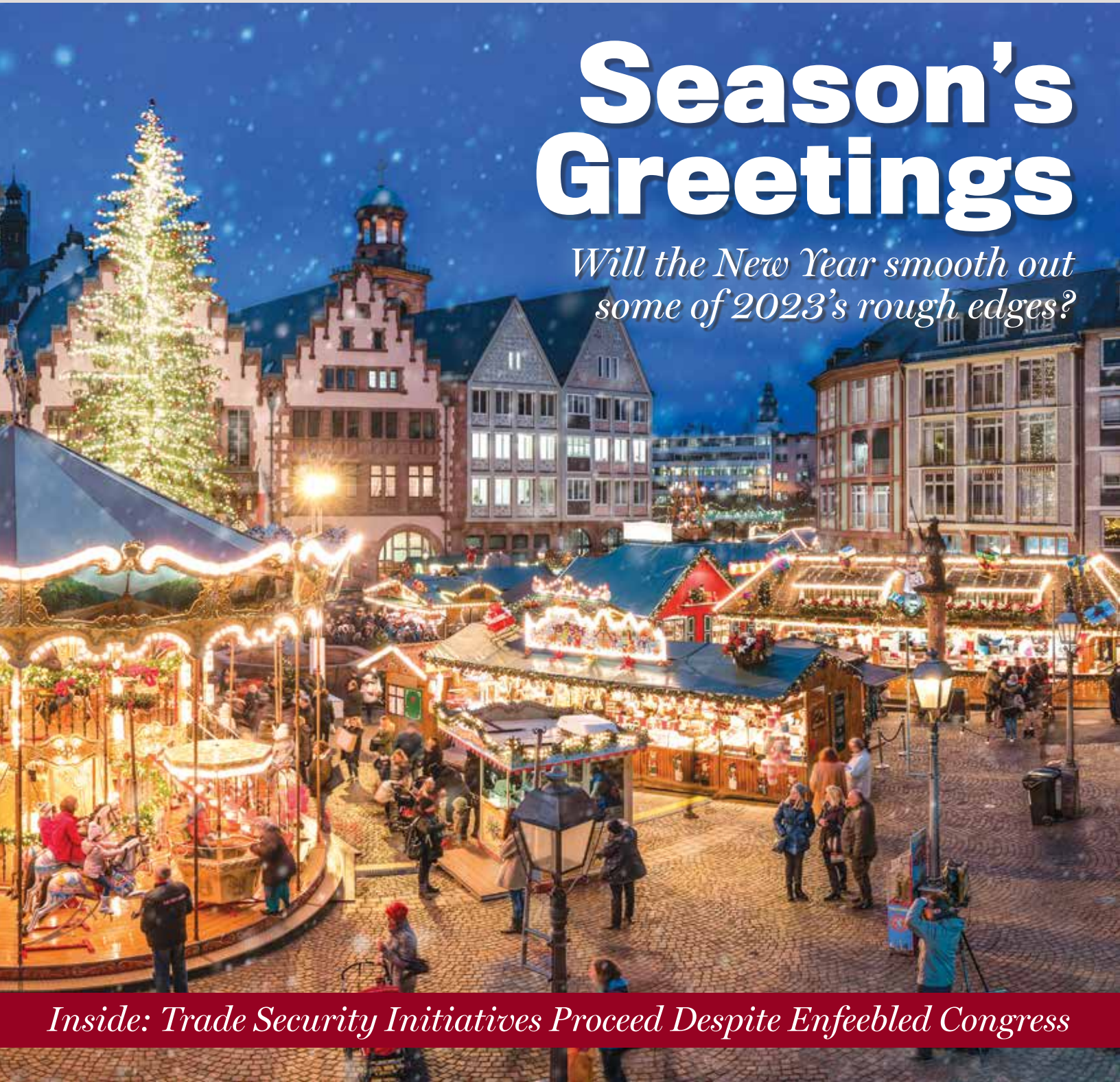
December 2023 | Vol. 37, No. 12

EP THE EXPORT PRACTITIONER™

IN THIS ISSUE:



Season's Greetings

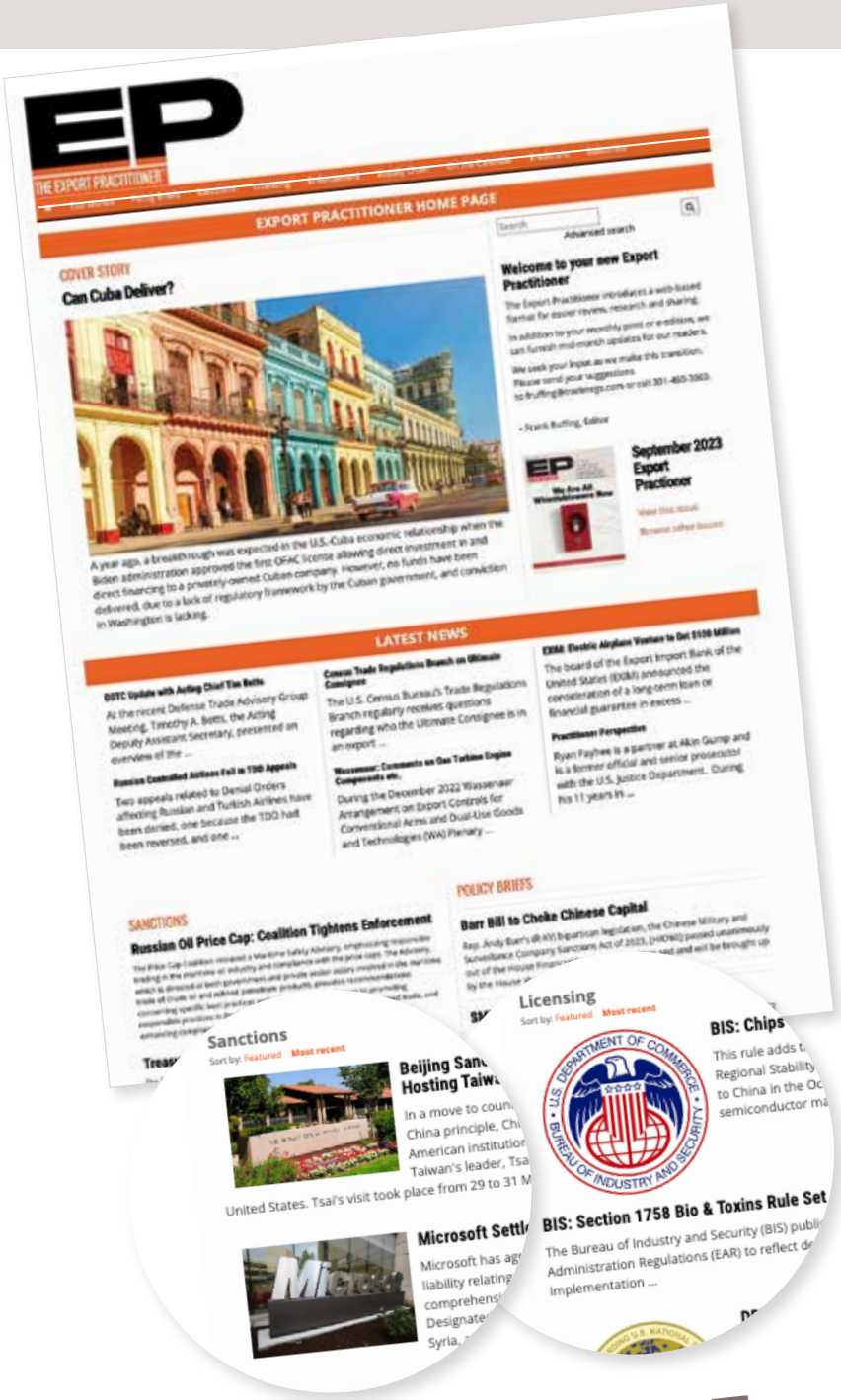
Will the New Year smooth out some of 2023's rough edges?

Inside: Trade Security Initiatives Proceed Despite Enfeebled Congress

WELCOME TO YOUR NEW

EXPORT PRACTITIONER™

IN PRINT | VIA EMAIL | ONLINE



VISIT ONLINE AT EXPORTPRAC.COM

FROM THE EDITOR:

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

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

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

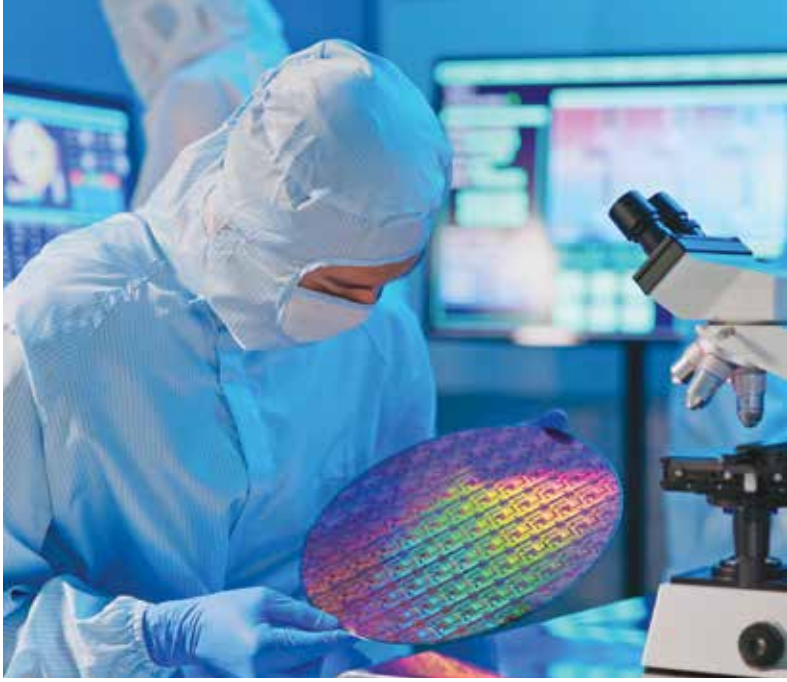
Share your thinking with the Export Practitioner community

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

TO SUBSCRIBE, OR TO SUBMIT CONTENT:
Contact Editor Frank Ruffing at fruffing@traderegs.com, or call 301-460-3060.

Scan or Click For Our Top Stories:

EP
THE EXPORT PRACTITIONER™
December 2023 | VOL. 37, NO. 12



RYANKING999 / ADOBESTOCK

FEATURE

POLICY

FOCUS ON ENFORCEMENT

EXPORT CONTROLS

SANCTIONS ROUNDUP

ON THE COVER: Christmas market, Frankfurt, Germany. EYETRONIC / ADOBESTOCK

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.

ISSN 1087-478K

FEATURE

GORODENKOFF/ADOBESTOCK

'So how are we going to build chip production in the United States, where we have assured supply? Semiconductors are the foundation of a lot of what goes on in our economy.'

Estevez at CSET: Export Controls at Inflection Point

In a wide ranging conversation at Georgetown University, Under Secretary of Commerce for Industry and Security Alan Estevez shared his perspective on the evolution of export controls and the road ahead. [*Excerpts edited for clarity*]

"I believe now that we are at sort of a foundational inflection point as to the role and purpose of export controls," Estevez said. "Commerce is in the middle of national security in a number of spheres these days.

"We do it from two perspectives. We do it from offense and we do it from defense. Offense is things like Chips Act. So how are we going to build chip production in the United States, where we have assured supply? Semiconductors are the foundation of a lot of what goes on in our economy.

"Again I said assured supply, not sufficient supply because we're still going to rely on [others] for providing semiconductors. That includes potentially adversarial nations we're trying to wean ourselves away from. "And it's not just semiconductors. It's working through things like the TTC in our work with Europeans or IPEF for work with our Asian allies around things like reworks and supply chain issues. There's lots of other things that could happen.

So if COVID didn't wake you up, Putin's invasion of Ukraine should have taught you not to unreliable on single source supply. We need to have diverse supply, and those are the things that we're working on.

'So if COVID didn't wake you up, Putin's invasion of Ukraine should have taught you not to rely on single source supply.'

ALAN ESTEVEZ, UNDER SECRETARY OF COMMERCE FOR INDUSTRY AND SECURITY

"The core of the defense structure is our export controls. Protecting the technology that our adversaries could use against us, should it ever come to any kind of kinetic action.

The Chinese have their sovereign nation. **They can modernize their military. There's nothing that the United States can really say to prevent that. They can modernize their military, they just can't do it with our stuff. Our stuff or our allied stuff?** And that's the goal that we're trying to achieve in our export controls.

There is impact in the economy, but that's not the goal. So the goal remains the same to impede Chinese military modernization. I think we need to be realistic that it is not stop. Stop is pretty much an impossibility. So all we're doing is putting up impact time. It's time and it's money. It's going to cost them more and it's going to take them longer to achieve the same outcome.

"[In Russia] the analogy I like to use is an Anaconda. It's going to slowly squeeze the life out of the Russian industrial base. Probably not fast enough for the Ukrainians. We are slowly going to squeeze the life out of the Russian defense industrial base. I'll know I'm successful when they're throwing rocks on the front line there.

"I talked to companies all the time. No company wants to be told I'm going to shave revenue from them. Most of them understand the rationale of why we're doing it. Most of them, they'll comply. They're all really good American companies, They're all going to apply. Uh. They might not be happy.

"Companies are going to do what companies do. Companies are in the business of making profit for them and their shareholders. That what drives the innovation in the American system. It's a good system. We support that system where I want that innovation, that innovation is key, not just to run faster for defense, it's key for the underpinning of the American economy and the economy of our allies. And we want that. So we're we encourage companies to go out and innovate.

Peripheral States

Bringing together countries to put controls on, Russia, we've had varying degrees of success in different countries. Countries in Central Asia where we see companies that didn't exist till March 2022 that are now on the receiving end of weird trade like, you know, 12,000% increase in laptops going to Armenia, where there hasn't been a 12,000% increase in population. We're going into those countries. I've met with ministers of all these countries. We've sent teams out with Treasury as well.

I know when I meet with them that they live in a very tough neighborhood. And that now a state on their border seems to think that any state that had SSR on the end of it belongs to it. So you gotta recognize that. But we also tell them there's a problem. You take care of it, or we will. And so it's whack A mole. Gotta keep on.

What's Next?

[With Russia] we're sort of out of bullets on what else we can do. You know we can go full embargo. Our goal has never been to harm the Russian people per se. Like stopping medicines from going has its own negative effect.

China is a harder question. There's it's hard question for us too. The economies are intertwined. Where do you make the most impact and what's the negative consequence of that impact? Sometimes that trade space impacts our national security too.

We have some proposals in Wassenaar related to quantum, again and are going to propose it this

Continues on next page

Continued from previous page

year that Russia's gonna not vote for. Wassenaar is a consensus organization. Wassenaar is going to operate under a consensus -1 capability.

Biotech is another area, especially areas like synthetic biology, which have all sorts of upsides and downsides. The trick on areas like biotechnology is, one, what's my choke point that I'm really going to go after? Is it widely available or is it really a choke point?

And two. I'm not trying to impede the PRC from curing cancer. That's good for mankind, Sometimes those same machines do this and do that.

Recruiting Talent

I am working to beef up technological capability, both internal and external to BIS. We need tech inside BIS. In the DoD world, where we never had enough money, we had a lot of money. So I'm always gonna go back: I need resources to do this job better. I need to build out that capability. I want to see BIS using 21st century tools when I leave.

I'd like to have like the DARPA model in the BIS. It would be hard to do that because DARPA has separate hiring authorities, and people in DARPA, roll in and out of government. They come in from whatever lab, academia or company that they're working at on this very hard problem. And then we say, hey, come to DARPA and we're going to give you an even harder problem in your field of study. But it's going to be the coolest thing you ever work on your life. They want to come do that for four or five years, and then they go back.

Coming and saying, hey, I want you to come in here so you can explain to me how I can regulate this technology, right? Nonetheless, again, my secretary says she's working to make BIS the most important fun place to work in government. And I'm all in on that role. And so we're looking for smart people. [11515]

House Panel Grills BIS Leaders

"DON'T TRY TO BULLSHIT A BULLSHITTER," admonished **Chairman Brian Mast** (R-FL), as **Assistant Commerce Secretary for Export Administration Thea Kendler** responded to his subcommittee's questions on decision making in the Bureau of Industry and Security.

Observers who thought Oversight and Accountability Subcommittee of the House Committee on Foreign Affairs hearing "*Reviewing the Bureau of Industry and Security, Part II: U.S. Export Controls in an Era of Strategic Competition*," with Ms. Kendler and **Assistant Secretary for Export Enforcement Matt Axelrod** would inform the conversation on enforcement priorities and resources may have been disappointed Dec. 12, as the committee's questioning centered on a deal removing China's Ministry of Public Security's Institute of Forensic Science (IFS) from the entity list.

Fentanyl precursor chemicals were being sent to the U.S. from China.

DARWIN BRANDIS / ADOBE STOCK

Institute of Forensic Science (IFS)

IFS was placed on the list in May 2020 for being "complicit in human rights violations and abuses committed in China's campaign of repression, mass arbitrary detention, forced labor and high-technology surveillance against Uighurs, ethnic Kazakhs, and other members of Muslim minority groups in the Xinjiang Uighur Autonomous Region. "The delisting was the product of a horse trade between the Justice Department (DEA), Homeland Security (ICE) and Beijing to obtain cooperation in stemming the flow of Fentanyl precursors chemicals from China.

Ms. Kendler was candid about why a notorious keystone in China's police state was given a pass: "It became clear to us that including IFS on the Commerce departments entity list was inhibiting the counter narcotics action that we thought

was necessary."

In response to continued questioning, Mr. Axelrod pulled no punches: "Look, I think it's fair to say that there are whenever there's a delisting decision, it's a variety of factors come into play. In some circumstances it can be more narrowly targeted to the particular entity and whether the particular entity has changed its behavior In other circumstances, such as this one, the delisting decision can rely less on the specific entity that was delisted and more on other factors that also need to be taken into account...

"100,000 people are dying a year from fentanyl. I was a drug prosecutor in Miami, and I prosecuted the Cali cartel. At its height, the Cali cartel was sending more cocaine into this country than anywhere anyone else ever in history. But cocaine wasn't killing people the way Fentanyl is. We have to do everything in our power, use all our tools to help save American lives. This was a decision that that we believe will help do that, and that's why it was done.

"The issue here was that the listing of IFS was a consistent impediment to getting agreement from the Chinese to take specific actions to help with the fentanyl crisis, to help make sure that precursor chemicals weren't being sent from China."

Firearms Export License "Pause"

In response to **Rep. Tim Burchett** (R-TN) Ms. Kendler downplayed the industry impact of the Bureau's 90 day "pause" in firearms exports:

"Congressman, our pause on firearms licensing applies only to commercial entities outside of our close partner countries, including Israel and Ukraine. That temporary pause, which we're halfway through at this point, is based on national security and foreign policy considerations. During this pause, we are using the time to figure out how best we can align our policy with our national security priorities.

"We're looking at this from national security and foreign policy angle. I would particularly point to our authorizing statute ECRA which calls that we look at regional stability issues and and particularly in the Western Hemisphere we we have gun violence issues that lead to regional instability. The during the pause we are very much consulting with stakeholders.

"NATO license applications are still being processed at the frankly that's about 75% by value of our license applications that we are continuing to process.

Funding for BIS

Rep. Andy Kim (D-NJ) asked what impact the Republican proposed 40% cuts to the Department of Commerce budgetwould have on BIS's work.

"Look, a cut to our budget would directly impact our national security work. It will affect our ability to aggressively enforce the expanding controls that have been put in place on Russia and and China. The Ukraine supplemental that you all were kind enough to pass gave us new resources that were added to our base in fiscal year 23, including fourteen new special agents and ten new intelligence analysts and support personnel.

"If we were to go back to our fiscal year 22 levels, it would cut 10% of our agents at a time when the need for more agents has never been higher. So I would, I would urge the committee not to not to cut us. If anything, we can always do more with more," Ms. Kendler said.

Ranking member Jason Crow (D-CO) asked what the Bureau would do with more resources. "Our our mission is harder and more complex given the evolving technology space," replied Ms. Kendler.

"I think I'd start with the the office of international policy and building up technical analysis of the emerging technologies... We put more resources into the licensing so that we can provide a faster response in reviewing license applications while committing the same efforts to protecting national security and foreign policy interests.

"We would beef up the resources we relied upon for open source information in foreign languages...it would enable us to look at what other countries, adversaries are publishing in their own materials about their goals, where they're spending their sovereign wealth, how they are investing in technologies in a way that may not be clear if you just follow US sources or or English language sources. It would also enable us to develop controls more carefully in collaboration with international partners and allies."

Mr. Axelrod too had a ready ask: "For us, three things:

• More agents I mentioned the disruptive technology strike force we would be able to put more agents against. Doing investigations, particularly involving China and Russia.

• Second, more analysts. We don't currently have enough analysts to have them embedded in our field offices around the country. If we had more resources, we would make sure that each of our field offices had an analyst working there alongside the agents.

• And third we'd invest in technology tools. One way to magnify the efficiency and effectiveness of the people we do have is through technology. If we have more resources, we could buy some of those technology tools to allow us to do our work smarter.

[11510]

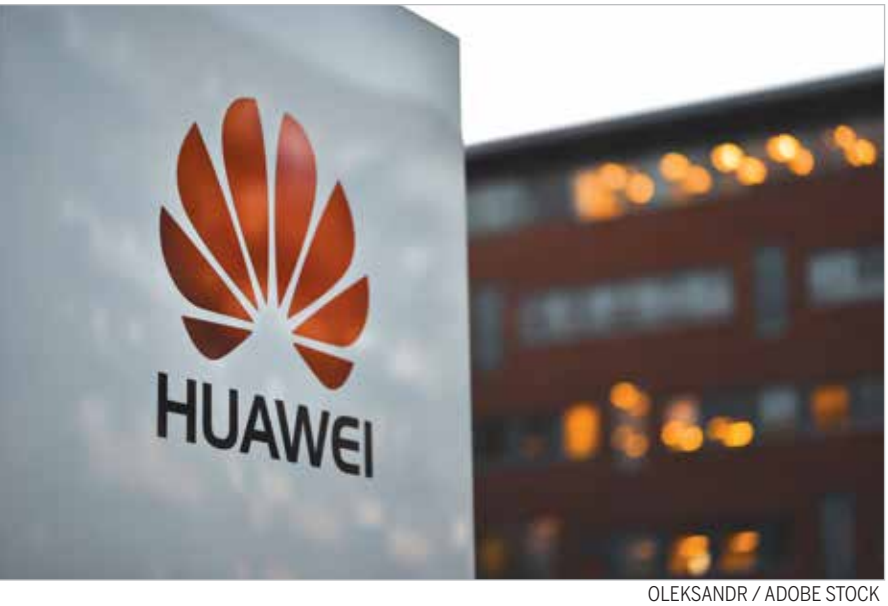
Congress Weighs in on BIS Reform

Following Commerce Secretary Gina Raimondo's call for additional funds for the Bureau of Industry and Security, Republican members of Congress called for a harder line on China first.

House Foreign Affairs Committee Chairman Michael McCaul (R-TX), House Republican Conference Chair Elise Stefanik (R-NY), and House Select Committee on the Chinese Communist Party Chairman Mike Gallagher (R-WI) released the joint statement below:

"Before we agree to work with Secretary Raimondo to provide additional resources to the Bureau of Industry and Security, the Department of Commerce must institute necessary reforms to keep U.S. technology from our adversaries. Resources alone will not address the shortcomings in our export control regime.

"Revoking Huawei licenses, adding BGI and Inspur subsidiaries to the Entity List, or cutting SMIC off from U.S. technology is not a matter of money, but political will. Any conversation about additional resources must be matched with actions that demonstrate BIS is being reformed into a true national security agency that will do what needs to be done to counter China and other adversaries."



OLEKSANDR / ADOBE STOCK

Republican members of Congress want to enforce a "policy of denial" for all U.S. technology exports to PRC firms involved in espionage, including Huawei and ZTE

Gallagher Committee Reports

Following a year of hearings and demands for reams of disclosure from government and industry, the House Select Committee on China released its work product for 2023.

The 53 page report enumerated recommendations to address Beijing's human rights violations and military modernization, focusing on halting the genocide of the Uyghur population and curtailing profits from forced Uyghur labor. Additionally, it aims to build a more credible deterrent in the Taiwan Strait.

The report presents findings and recommendations, outlining a strategy to compete with the PRC in economic and technological spheres. The strategy is based on three pillars.

Resetting the U.S.-PRC Economic Relationship:

- **Key Finding:** The PRC's economic system is not compatible with WTO standards, undermining U.S. economic security. The strategy involves revisiting the PRC's trade status and advocating for annual renewal of trade relations.
- **Recommendations** include countering the PRC's economic strategies, increasing transparency in U.S. investments in the PRC, preparing for economic impacts of potential conflicts, and

protecting U.S. markets from PRC products that distort the market.

• "It is time for likeminded countries to come together and seriously examine how to collectively counter the PRC's approach to economics and the harm it is doing to the global trading system," the report authors write. "If this cannot be achieved within the confines of the WTO, then a new multilateral effort by likeminded market economies that goes back to first principles is needed"

Stemming the Flow of U.S. Technology and Capital to the PRC:

• **Key Finding:** American investors wittingly and unwittingly support the PRC's defense industry and human rights abuses.

• **Recommendations** focus on restricting investments in entities associated with the PLA, critical technology sectors, or forced labor.

• **Strengthening export controls** to restrict critical technology transfer to the PRC and modernizing export controls to adapt to rapid technological changes and the PRC's Military-Civil Fusion strategy are also suggested.

Investing in U.S. Technological Leadership and Economic Resilience:

• **Key Findings and Recommendations** involve investing in American innovation, executing a talent strategy for R&D in critical technologies, developing a positive economic agenda with allies, increasing transparency in U.S. dependency on critical minerals from the PRC, reducing dependency on the PRC for pharmaceutical supply chains, and expanding tools to counter the Belt and Road Initiative through strategic investments and reforms.

Export Control Specifics

To enhance national security, Congress is advised to implement the following measures:

Allocate Additional Resources to the BIS:

• Enhance the Bureau of Industry and Security (BIS) within the Commerce Department with increased personnel, technology, data management, and intelligence support.

• Implement necessary reforms, such as updating the End User Review Committee's process, closing the "subsidiary loophole," and expanding BIS's authority over dual-use open-source technology.

Implement Country-Wide Controls:

• Adopt "country-wide" controls similar to those applied to advanced semiconductors on Oct. 7, 2022.

• Require the Department of Commerce to establish these controls for specific technologies sent to foreign adversaries, enforcing a "policy of denial" for export licenses on items under "National Security" controls.

Establish Comprehensive Controls on Critical Technologies:

• Mandate quick establishment of general controls on critical and emerging technologies exported to foreign adversaries, including AI, quantum technologies, biotechnology, advanced materials, optics, energy research, and space-based technologies.

Expand Export License Requirements:

• Broaden export license requirements to include subsidiaries of foreign adversaries on the Entity List to prevent technology diversion.

Conduct Comprehensive EAR-99 Review:

• Instruct the ERC to thoroughly review all commercial items (EAR-99) for potential export control applicability.

• Authorize the Departments of Defense, State, and Energy to nominate EAR-99 items for control based on national security or foreign policy reasons.

Establish Cloud Computing End-Use Rule:

• Direct the Department of Commerce to set a rule for cloud computing end-uses, limiting U.S. technology in advanced cloud computing clusters for foreign adversaries.

• Implement "know-your-customer" requirements for U.S. cloud computing firms and mandate reporting to the Commerce Department on significant computational resource rentals by foreign adversary companies.

Implement Policy of Denial for PRC Firms:

• Enforce a "policy of denial" for all U.S. technology exports to PRC firms involved in espionage, including Huawei and ZTE, and revoke existing licenses.

• Prohibit export control licenses for products and technologies related to supercomputing for specific PRC entities.

Negotiate Expanded Multilateral Controls:

• Instruct the Department of State, alongside the Multilateral Action on Sensitive Technologies group and the Department of Commerce, to negotiate expanded controls with democratic partners on key technologies.

• Collaborate with NIST and the Department of Energy to set international standards in artificial intelligence.

Establish a New Plurilateral Export Control Regime:

• Direct the Department of State to create a new export control regime, modeled after COCOM, including like-minded partners and allies.

• Focus this regime on preventing PRC and other foreign adversaries' access to critical and dual-use emerging technologies.

• Provide incentives and resources for countries to participate in this new export control framework. [11483]

Foreign Affairs Chimes In

A REPORT BY THE HOUSE FOREIGN AFFAIRS Committee highlights shortcomings in the U.S. export control system and calls for reforms, legislative and administrative. Drawing extensively on the work of former Defense Department Export Control Official Stephen Coonen, the report reflects the chilly reception BIS receives in the House of Representatives..

"Both the Trump and Biden administrations, principally from the White House, have rightly begun exerting more control over the Commerce Department's Bureau of Industry and Security (BIS). However, no administration will be able to fully leverage the power of export controls to protect U.S. national security without Congressional action. Now, Congress must solidify the efforts of successive administrations so our future will be better secured," the authors assert.

Central to the committee's findings is the concern that BIS, under the Commerce Department, has been too lenient in granting licenses for dual-use technology transfers to China, failing to adequately consider the likelihood of military or surveillance use.

"Through the bipartisan *Export Control Reform Act of 2018* (ECRA) and recent legislative updates, Congress has given BIS tremendous authority to stop, or at least slow down, technology diversion to the CCP's military or surveillance state. Despite Congress passing ECRA and empowering BIS to draft new regulations to address unique features of China's economy, including MCF, the bureau has not aggressively or proactively done so Rather, it is maintaining a reactive approach, generally responding only after a crisis occurs."

Emerging & Foundational Technologies

In addition to reported failures, BIS has not implemented key portions of ECRA, including identifying emerging and foundational technology and reviewing license requirements through the lens of MCF (China's Military-Civil Fusion). A statutory requirement in ECRA Section 1759 to review controlled items based on MCF apparently achieved nothing, because no new controls have been issued. A statutory requirement in ECRA 1758 to identify emerging and foundational technology has resulted in zero foundational technology controls."

HFAC majority staff contends that BIS struggles to achieve its national security mission because it sits within the Department of Commerce, which is designed to increase exports.

According to Chairman McCaul the export control regime must evolve on two simultaneous tracks.

First, The bureau needs major reforming to ensure the national security mission is not undermined by countervailing goals — such as export promotion.

Second, the export control regime needs immediate modernizations to limit, and ideally stop, the hemorrhaging of sensitive U.S. technology to China.

Reforms

The report highlights several problems and recommendations:

Operating Committee Voting System: The committee suggests adopting a majority vote system for license reviews.

BIS Regulations Compliance: Mandate BIS refer license applications to other appropriate agencies, including Defense, Energy, and State, for items that implicate their interests (e.g. Defense reviews items controlled for national security and Energy

reviews items controlled for nuclear non- proliferation).

Policy of Denial: recommend that BIS adopt a "policy of denial" or "presumption of denial" license review standard for all licenses to export items controlled for national security reasons to China

EAR99 Technologies Review: BIS should reassess technologies designated EAR99 and adjust controls on the Commerce Control List.

Entity List and End-User Controls: Apply a presumption of denial for items subject to the EAR for companies on the Entity List, and expand Entity List Coverage.

Unlike the Department of the Treasury Office of Foreign Asset Control's 50 Percent Rule, BIS typically designates a specific affiliate of a company instead of the entire corporate structure, including subsidiaries and affiliates. Identifying one subsidiary at a time, "ignores the reality that the entire corporate system in the People's Republic of China ("PRC") is encouraged—and often mandated — by the PRC government to circumvent U.S. laws."

Military End-User Rule: BIS should adopt a standard definition of a Chinese military company.

Plurilateral Export Controls: Drawing on the lessons of the Cold War's Coordinating Committee for Multilateral Export Controls (CoCom), the U.S. should pursue agreements with allies to control specific emerging technologies.

Strengthened End Use Checks and Oversight: Address the high "willfulness" standard for criminal prosecutions, improve end-use checks, and enhance oversight. Congress should legislate a new standard for criminal prosecutions to support enforcement actions that deter future evasion or violations. Commerce must renegotiate its end-use agreement with the PRC or impose greater restrictions on exports to China considering the inability to conduct meaningful end-use checks.

Fundamental Research Policies: Reform NSD-189 to address China's acquisition of technology through fundamental research.

"Universities, research institutes, government laboratories and others routinely look to the fundamental research exception in the EAR (§ 734.7) to eliminate export licensing requirements for cross-border activities."

NSD-189 must be reformed by the Biden administration to address China's acquisition of critical technology and know-how through fundamental research and Congress must put adequate safeguards on fundamental research.

BIS Resources and Personnel: Amend ECRA to allow BIS to charge fees on certain licenses to support enforcement efforts. "The Bureau of Industry and Security appears not to have prioritized hiring people with the linguistic, technical, or geopolitical expertise needed to carry out its mission."

'Is Informed' Letters: Address concerns about BIS's use of 'is informed' letters. "The letters give the appearance of acting without certainty that transfers are in fact being stopped. There is concern that BIS is using these 'is informed' letters to prevent other agencies from taking more consequential actions."

Standard-setting activities. In Sept. 2022, BIS issued an interim final rule to authorize the release of items subject to export controls without a license, including to companies on the Entity List, so long as that release occurs in the context of a "standards-related activity."

Because almost any exchange between two or more entities could be self-classified as a "standards-related activity," BIS created a dangerous loophole that removes any U.S. government visibility into sensitive technology transfers and undercuts Entity List enforcement. [11483]

China Commission Calls for Single Export Control Regime

CONGRESS SHOULD CONSIDER CREATING a single export licensing system to strengthen export controls on China, the bipartisan U.S.-China Economic and Security Review Commission said in its annual report to Congress.

The Administration has taken steps to impose a tough export control regime on China in order to prevent Beijing from accessing U.S. technology in order to gain an edge over the United States in emerging technologies that have potential national security concerns. In its report, the commission urged Congress to consider a number of steps to make it more difficult for China to evade U.S. controls.

First, the report recommends that Congress hold hearings to evaluate the potential for establishing a single export licensing system. Such a system would integrate the Commerce Control List, the dual-use technology licensing system managed by the Commerce Department's Bureau of Industry and Security and the U.S. Munitions List, the armaments licensing system managed by the State

Continues on next page

Continued from previous page

Department's Directorate of Defense Trade Controls.

In evaluating a single licensing system, the commission said Congress should consider:

• Whether a single licensing system could improve the enforcement of export controls targeting specific end users, particularly those in jurisdictions with poor transparency into corporate ownership and commercial affiliations, such as China;

• The potential commercial impact of combining the licensing systems, including how to reduce the compliance burden on industry without compromising national security;

• Which technologies to include in a combined system and how to integrate appropriate technical expertise to scope evolving controls on dual-use emerging and foundational technologies;

• Where such a system should be housed within the US government and how to establish effective coordination between different agency stakeholders and

• How to provide the Department of State and other relevant agencies with appropriate information and authorities to advocate for multilateral export controls that advance US security, foreign policy and economic competitiveness.

The report also suggests that Congress provide the **Committee on Foreign Investment in the United States** the authority to review investments in US companies that could support foreign acquisition of capabilities to attain technological self-sufficiency or otherwise impair the economic competitiveness of the United States, including:

• Investments in technology areas prioritized in potential adversaries' industrial policies, such as China's 14th Five-Year Plan, Made in China 2025, and other related initiatives;

• Investments in US firms that have received funding from the Defense, Commerce, Energy and other US government funding for projects critical to national security and competitiveness and

• Other investments that may provide privileged access to expertise, business networks and production methods critical to maintaining US economic and technological competitiveness.

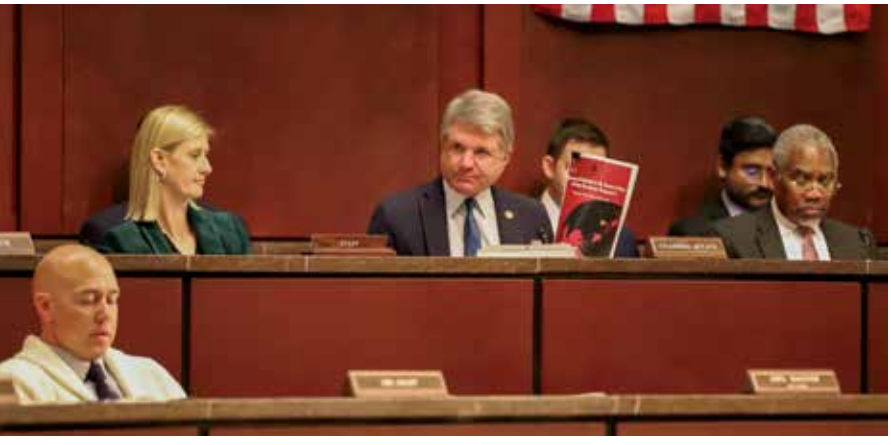
The report also proposes that Congress establish a risk matrix framework to evaluate the national security threat posed by electronic products imported from China. To eliminate or mitigate risks identified in the threat matrix evaluation, Congress should consider the use of all trade tools, including tariffs.

In addition, Congress should request an evaluation, to be completed within 180 days by the General Accountability Office, of the effectiveness of recently imposed semiconductor export control regulations in preventing China from either acquiring or developing the capacity to manufacture certain advanced semiconductors.

The report is part of the Commission's mandate to investigate, assess, and report to Congress annually on "the national security implications of the economic relationship between the United States and the People's Republic of China." [11409]

House Foreign Affairs Marks Up Export Control Bills

Chairman McCaul conferring with Rep. Mast



AFTER A YEAR of limited productivity, Congress decided to get some work done in the last working week of the year. The House Foreign Affairs Committee Chairman held a markup session to consider various measures regarding export controls, restricting the flow of foreign nations' support to the Taliban, and strengthening sanctions against Hamas, Palestinian Islamic Jihad and other terrorist groups on Wednesday, Dec. 13, 2023.

Export Contol Related Legislation

H.R. 6602, To amend the Export Control Reform Act of 2018 relating to the review of the interagency dispute resolution process; Enhancing the role of the Departments of Defense, State, and Energy by granting them equal voting rights in the export controls licensing committee led by the Commerce Department, with the Bu-

reau of Industry and Security (BIS) retaining the power to resolve any ties.

H.R. 6606, To amend the Export Control Reform Act of 2018 relating to the statement of policy; Requiring BIS to regularly update Congress every 90 days on its licensing decisions and other export control enforcement actions.

H.R. 5613, To require a review of whether individuals or entities subject to the imposition of certain sanctions through inclusion on certain sanctions lists should also be subject to the imposition of other sanctions and included on other sanctions lists; Promoting coordination between BIS, the Departments of Defense and Treasury in aligning their respective trade restriction lists, along with a mandate to justify to Congress any discrepancies in sanctions against entities.

H.R. 6614, To amend the Export Control Reform Act of 2018 relating to licensing transparency; Expanding BIS's duties to encompass the safeguarding of trade secrets. [11512]

AUKUS

Defense Chiefs Announce Pillar II Initiatives

DEFENSE CHIEFS of the AUKUS military-industrial alliance met at the Defense Innovation Unit Headquarters at Moffett Field in California to discuss progress for the partnership, especially Pillar II, the broad based defense industrial collaboration.

Defense Secretary Lloyd Austin was joined by Australian Deputy Prime Minister Richard Marles, who also serves as defense minister, and British Defense Secretary Grant Shapps. The defense chiefs saw capability demonstrations focused on artificial intelligence, integrated air defense systems, tactical augmented reality, space architecture and virtual training for air dominance.

"[A] watershed in the progress of Pillar II of AUKUS," Marles called the meeting. "AUKUS represents a powerful combination of countries working together, which is sending a really important message to the world,"

A senior defense official said that AUKUS is collaborating on artificial intelligence, autonomy, advanced cyber, electronic warfare, hypersonics, counterhypersonics, quantum technologies and undersea warfare.

The three nations are also establishing an AUKUS Industry Forum with trilateral government and industry representatives to help inform policy, technical and commercial frameworks to facilitate the development and delivery of advanced capabilities. The initial meeting of that forum will occur in the first half of 2024.

In a Joint Statement, the Secretaries and Deputy Prime Minister reaffirmed the three nations' commitment to maximize the strategic and technological advantage of AUKUS . They agreed that advancing AUKUS requires continued commitment to streamlining defense trade controls and information-sharing while minimizing policy and financial barriers across public and private sectors

Pillar II — Advanced Capabilities

Pillar II is facilitating collaboration in advanced technologies. In addition to work focused on dedicated AUKUS capabilities, AUKUS is providing a vehicle to break down barriers and improve cooperation in other areas. While many AUKUS-related advanced capability activities remain classified, the Secretaries and Deputy Prime Minister shared the following commitments:

• **AUKUS Maritime Autonomy Experimentation and Exercise Series.** The AUKUS partners will undertake a series of integrated trilateral experiments and exercises aimed at enhancing capability development, improving interoperability, and increasing the sophistication and scale of autonomous systems in the maritime domain. Through these experiments and exercises, the AUKUS partners will also further test and refine the ability to jointly operate uncrewed maritime systems, share and process maritime data from all three nations, and provide real-time maritime domain awareness to support decision-making.

Trilateral Anti-Submarine Warfare. The AUKUS partners will deploy common advanced artificial intelligence (AI) algorithms on multiple systems, including P-8A Maritime Patrol Aircraft, to process data from each nation's sonobuoys. These joint advances will allow for timely high-volume data analysis, improving our anti-submarine warfare capabilities.

Undersea Vehicle Launch and Recovery. The AUKUS partners are integrating the ability to launch and recover undersea vehicles from torpedo tubes on current classes of submarines to deliver effects such as strike and intelligence, surveillance, and reconnaissance.

Quantum Positioning, Navigation, and

Continues on next page

Continued from previous page

Timing. The AUKUS partners are accelerating the development of quantum technologies for positioning, navigation, and timing in military capabilities. These capabilities create resilience for our trilateral forces in Global Positioning System-degraded environments and enhance stealth in the undersea domain.

Resilient and Autonomous Artificial Intelligence Technologies (RAAIT). The AUKUS partners are delivering artificial intelligence algorithms and machine learning to enhance force protection, precision targeting, and intelligence, surveillance, and reconnaissance. This effort builds on joint work demonstrated in the UK in April 2023 and in South Australia in October 2023.

Deep Space Advanced Radar Capability. AUKUS is accelerating capabilities that provide trilateral partners with advanced technology to identify emerging threats in space. The Deep Space Advanced Radar Capability program, will provide 24-hour continuous, all-weather global coverage to detect, track, and identify objects in deep space and increase space domain awareness. Sites will be in the United States, United Kingdom, and Australia. The first radar site in Western Australia will be operational in 2026, with all three in service by the end of the decade.

Cyber. Trilaterally, AUKUS partners are engaging on cyber security with critical suppliers to the naval supply chain. We are collaborating with industry partners to deploy some advanced tooling which will uplift the cyber security of our supply chains, while also giving us greater insight into the threats to AUKUS. The AUKUS partners are also working to strengthen cyber capabilities, including protecting critical communication and operations' systems.

Establishing Trilateral Requirements. The Secretaries and Deputy Prime Minister noted that the International Joint Requirements Oversight Council, co-chaired by the Vice Chiefs of Defense from the United States, the United Kingdom, and Australia, is a key collaborative forum.

AUKUS Innovation Challenges. AUKUS partners will launch a series of AUKUS innovation challenges in which companies from across all three innovation ecosystems will be able to compete for prizes on a common innovation challenge topic. In early 2024, partners will launch the first trilateral Innovation Prize Challenge, focusing on electronic warfare.

Defense Trade and Industrial Base Collaboration. The AUKUS partners are working to facilitate deeper and more rapid defense trade between the three nations by streamlining policies and processes, along with implementing comparable security standards for guiding the transfer of sensitive military technology, data, and know-how. .

AUKUS Advanced Capabilities Industry Forum. The AUKUS partners will establish and convene a standing Industry Forum with trilateral government and industry representatives to help inform policy, technical, and commercial frameworks to facilitate the development and delivery of advanced capabilities. The first meeting will occur in the first half of 2024.

AUKUS Defense Investors Network. The AUKUS partners are increasing and expanding private sector engagement by welcoming the creation of an AUKUS Defense Investors Network, leveraging the current networks in all three countries to strengthen financing and facilitate targeted industry connectivity.

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 for a photo opportunity in February 2019.

Pillar I — Conventionally Armed, Nuclear-Powered Submarines

The Secretaries and Deputy Prime Minister reviewed the progress that has been made since the March 2023 announcement of the Optimal Pathway for Australia to acquire conventionally armed, nuclear-powered submarines.

They reaffirmed their commitment to selling U.S. Virginia-class submarines to Australia from the early 2030s, and delivering SSN-AUKUS to the Royal Navy in the late 2030s and the first Australian-built SSN-AUKUS to the Royal Australian Navy (RAN) in the early 2040s. [11458]

CFIUS

Mexico Extension Envisioned

TREASURY SECRETARY JANET YELLEN, and Mexico's Secretary of Finance and Public Credit Rogelio Ramírez de la O signed a Memorandum of Intent to affirm the importance of foreign investment screening in protecting national security and express their desire to establish a bilateral working group for regular exchanges of information about how investment screening can best protect national security.

The MOI recognizes the importance of the U.S.-Mexico economic relationship, the benefits of maintaining an open investment climate, and the critical role of effective investment review mechanisms in addressing national security risks that can arise from certain foreign investment, particularly in certain technologies, critical infrastructure and sensitive data.

"I am pleased to announce our intention to establish a bilateral working group between the United States and Mexico on foreign investment review," Ms. Yellen said. "Both countries benefit when they work together to guard against foreign investments that pose national security risks. This engagement is further evidence of the close partnership between our two countries, not only on matters of trade but also on critical issues of national security."

North America faced significant supply chain challenges during the COVID-19 pandemic, and the U.S. and Mexico responded with new policy initiatives and approaches to bring jobs and investment in essential sectors back to the region. As this effort continues, cooperation between the U.S. and Mexico on investment security is one way to support shared national security objectives while promoting an open investment climate in the region, according to Treasury.

More than 20 countries implemented or enhanced their investment screening regimes in the past decade, and many more are in the process of developing regimes. A CFIUS-like arrangement with Mexico would aim to scrutinize foreign investments within Mexico, particularly those that might pose security risks.

Such a proposal would need to address the unique economic and security landscape of Mexico, considering its close economic ties with the U.S. and other nations. The challenge lies in striking a balance between safeguarding national security and maintaining a favorable investment environment. [11489]

BRIEFS

Pan E.U. Anti-Money Laundering Authority

➤ The European Council and the Parliament have reached a provisional agreement on creating a new European authority (AMLA) for countering money laundering and financing of terrorism. AMLA will have direct and indirect supervisory powers over high-risk obliged entities in the financial sector. It will monitor that those obliged entities have internal policies and procedures in place to ensure the implementation of targeted financial sanctions asset freezes and confiscations.

AMLA will have a general board composed of representatives of supervisors, Financial Intelligence Units from all member states, and an executive board composed of the chair of the authority and five independent full-time members.

The provisional agreement will be finalised and presented to member states' representatives and the European Parliament for approval. If approved, the Council and the Parliament must formally adopt the texts. [11505]

FCPA

International Corporate Anti-Bribery Initiative

➤ In a speech to the 40th International Conference on the Foreign Corrupt Practices Act, the Justice Department's FCPA Chief announced an anti-bribery initiative to drive cross-border collaboration in fighting foreign bribery.

Acting Assistant Attorney General Nicole Argentieri announced "a new resource in our fight against corruption: the International Corporate Anti-Bribery initiative, or ICAB, which will be driven by three experienced prosecutors, who will build on our existing bilateral and multilateral partnerships, as well as form new partnerships.

"Each member of this FCPA Unit initiative will work collaboratively, as appropriate, across the Criminal Division — including with MLARS, the Office of International Affairs, the Office of Overseas Prosecutorial Development, Assistance, and Training, and the International Criminal Investigative Training Assistance Program — as well as with colleagues in other parts of the department, our law enforcement partners, and the State Department.

"This is yet another reason companies considering whether or not to disclose misconduct should take note — call us before we, or our foreign partners, call you." [11466]

Oil Traders Pay $106 million to Settle Brazil Case

Operation Car Wash, the wide ranging graft case involving Petrobras officials and the commodity trading community snared another trophy culprit. Stamford, Conn.-based **Freepoint Commodities** agreed to pay the DOJ $98 million to resolve an investigation into bribery of Brazilian government officials. The firm has also agreed to pay more than $7.6 million to the Commodity Futures Trading Commission in a related matter.

Freepoint entered into a three-year deferred prosecution agreement with the department. The department reached this resolution with Freepoint based on a number of factors, noting: **"in the initial phases, Freepoint's cooperation was limited in degree and impact, and largely reactive."**

Remedial Measures

Freepoint also engaged in remedial measures, including:

• Conducting an analysis of the causes of the underlying conduct and undertaking appropriate remediation to address those root causes and taking additional steps to improve its compliance program, including by retaining an advisory firm to evaluate its third-party compliance program;

• Overhauling its third-party compliance and risk management program, including through the implementation of enhanced risk-based due diligence, screening, ongoing monitoring and oversight procedures, and the implementation of FCPA training for third-party agents;

• Reducing the use of third-party intermediaries;

• Implementing a global agent onboarding and tracking procedure;

• Strengthening its corporate governance and risk management structures, including through the utilization of data and metrics to evaluate risk, enhancing the independence and stature of its compliance function, and hiring additional, experienced compliance personnel;

• Updating the company's global anti-bribery and corruption policy to include FCPA red flags;

• Implementing a process for reporting and investigating allegations of misconduct; and

• Conducting testing of its third-party compliance program.

In light of these considerations, the criminal penalty calculated under the U.S. Sentencing Guidelines reflects a 15% reduction off the bottom of the applicable guidelines fine range. [11517]

JOAO SOUZA / ADOBE STOCK

China Cheating Costs PwC $7 Million

THE PUBLIC ACCOUNTING OVERSIGHT BOARD sanctioned **PwC China** and **PwC Hong Kong** for violating PCAOB quality control standards related to integrity and personnel management. Both firms failed to detect or prevent extensive, improper answer sharing on tests for mandatory internal training courses.

From 2018 until 2020, over 1,000 individuals from PwC Hong Kong, and hundreds of individuals from PwC China, engaged in improper answer sharing — by either providing or receiving access to answers through two unauthorized software applications — in connection with online tests for mandatory internal training courses related to the firms' U.S. auditing curriculum. The overwhelming majority of the professionals implicated in the answer sharing performed work for the firms' Assurance practices.

Without either firm admitting or denying the findings in the orders concerning the improper answer sharing, PwC Hong Kong was censured and agreed to pay a $4 million civil money penalty, and PwC China was censured and agreed to pay a $3 million civil money penalty. Both firms are required to review and improve their quality control policies and procedures to provide reasonable assurance that their personnel act with integrity in connection with internal training, and to report their compliance to the PCAOB within 150 days.

These are the first enforcement settlements with mainland Chinese and Hong Kong firms since the PCAOB secured historic access to inspect and investigate firms headquartered in China and Hong Kong in 2022. The sanctions include the highest civil money penalty the Board has imposed against a China-based firm and one of the highest penalties the Board has imposed against any firm.

The sanctions also include a requirement — for the first time ever in a Board disciplinary order — that a China-based firm retain an independent monitor.

Haoxin / Gridsum

The PCAOB sanctioned the accounting firm Haoxin and four of its associated persons for violations of the U.S. securities laws and PCAOB rules and standards in connection with the audits of the 2015-2017 financial statements of Gridsum Holding Inc.

ADOBE STOCK

Among violations, firm principals informed Gridsum that they expected to issue an unqualified opinion before Gridsum had actually engaged Haoxin as its external auditor.

Haoxin was censured and agreed to pay a civil money penalty of $750,000 and to accept immediate practice limitations, including prohibitions on accepting new PCAOB audit clients and a requirement for pre-issuance reviews.

Haoxin also agreed to remedial undertakings, including to retain (at the firm's expense) an independent monitor who will review and advise the firm on its policies and procedures, ensure the firm complies with the requirements of the order, and report back to the PCAOB.

Burner Phones in Hong Kong

The Financial Times reports that PwC peers Deloitte, KPMG and McKinsey have advised their U.S.-based executives not to use their work phones in the territory. This development illustrates the business community's perception of Hong Kong's security environment becoming one with the Mainland, where hacks and data security have long been suspect. [11455]

OFAC

Justice Target Serial Procurer for Russia

OFFICE OF FOREIGN ASSETS CONTROL (OFAC) is targeting a network led by Belgian serial offender **Hans De Geetere** involved in procuring electronics with military applications for Russian end-users.

Concurrent with OFAC's action, the U.S. Department of Justice (DOJ) unsealed two separate indictments against De Geetere related to his years-long scheme to unlawfully export sensitive, military-grade technology from the U.S. to end users located in the People's Republic of China (PRC) and the Russian Federation.

The U.S. Department of Commerce is also concurrently adding Hans De Geetere and five entities to the Bureau of Industry and Security (BIS) Entity List. Additionally, Belgian authorities took action against De Geetere on charges related to his global illicit procurement scheme.

Hans De Geetere and Companies

Hans De Geetere is a Belgian businessman and long-time procurement agent for Russia who serves as the director of several companies in Belgium, Cyprus, and the Netherlands. De Geetere has coordinated the procurement of electronics for Russian customers, including field programmable gate arrays (FPGA) — high priority semiconductor devices sought by Russia for its weapons programs.

De Geetere operates Belgium-based **Knokke Heist Support Corporation Management** (Knokke Heist), Cyprus-based **Eriner Limited** (Eriner), Cyprus-based **The Mother Ark Ltd** (The Mother Ark), and Netherlands-based **European Trading Technology B.V.** (European Trading Technology).

In some cases, De Geetere and his network have attempted to ship electronics to Russia via transshipment points in Hong Kong, China, and Türkiye.

Companies Linked to Eriner and the Mother Ark

In some cases, De Geetere and his network have attempted to ship electronics to Russia via transshipment points in Hong Kong, China, and Türkiye. The De Geetere-led company Eriner has repeatedly conducted business with the Hong Kong-based company M and S Trading, and coordinated electronics orders for Russia, including orders for integrated circuits of the same model as those identified in Russian-made unmanned aerial vehicles (UAV) recovered in Ukraine.

Individuals And Companies Linked to the De Geetere Network

In addition to the companies that he formally directs, De Geetere's network includes the Belgium-based company European Technical Trading (ETT), founded and led by his brother, Tom De Geetere. De Geetere has leveraged the ETT brand in attempted purchases from U.S. and European companies. In addition to his role as the founder and Director of ETT, Tom De Geetere has coordinated with his brother to procure UAV engines.

De Geetere has involved the Russian national Vladimir Kulemekov (Kulemekov) in multiple business dealings, including coordinating electronics orders for Russian entities. Kulemekov was previously employed by De Geetere and has been identified as a member of the previously designated Main Intelligence Directorate of the Russian General Staff (GRU).

In September 2022, De Geetere-controlled entity Hasa-Invest was added to the U.S. sanctions list, for procurement of dual-use accellerometers for China. This sanction was lifted after 180 days. The company declared bankruptcy later that year, having failed to report its financial results since 2014. De Geetere established a new company in Cyprus the following year. [11478]

UK Insurance Brokers Settle Ecuador Bribery Cases

TWO U.K.-BASED REINSURANCE BROKERS have agreed to resolve investigations by the Justice Department into violations of the Foreign Corrupt Practices Act (FCPA) arising from a corrupt scheme to pay bribes to Ecuadorian government officials. **Tysers** and **H.W. Wood** each entered into a three-year deferred prosecution agreement (DPA) with the department in connection with a criminal information filed in the Southern District of Florida charging both companies with conspiracy to violate the anti-bribery provisions of the FCPA.

"Tysers and H.W. Wood have admitted to engaging in a scheme to bribe multiple Ecuadorian government officials to earn tens of millions of dollars in illicit profits for themselves and their co-conspirators," said Acting Assistant Attorney General Nicole M. Argentieri of the Justice Department's Criminal Division.

According to court documents, between 2013 and 2017, Tysers and H.W. Wood, through their employees and third-party agents, agreed to pay bribes totaling approximately $2.8 million to the then-chairman of two Ecuadorian state-owned insurance companies, Seguros Sucre S.A. and Seguros Rocafuerte S.A., and three other Ecuadorian officials to secure improper advantages in order to obtain and retain reinsurance business with the state-owned insurance companies.

The bribes were paid to accounts held in Florida and elsewhere and effectuated through, among other things, emails sent from and meetings held in Florida. In furtherance of the scheme, Tysers paid approximately $20.3 million in commissions and H.W. Wood paid approximately $7.9 million in commissions and premium payments to the intermediary company that paid the bribes. Tysers retained commissions of approximately $10.5 million and H.W. Wood retained commissions of approximately $2.3 million.

Pursuant to the DPAs, Tysers and H.W. Wood have each agreed to continue to cooperate with the department in any ongoing or future criminal investigations relating to this conduct. In addition, Tysers and H.W. Wood have each agreed to continue to enhance their compliance programs and provide reports to the department regarding remediation and the implementation of compliance measures for the three-year term of the DPAs.

Tysers

Pursuant to its DPA, Tysers will pay a $36 million criminal penalty and administrative forfeiture of approximately $10.5 million. The department reached this resolution with Tysers based on a number of factors, including, among others, the nature and seriousness of the offense. Tysers received credit for its cooperation with the department's investigation, which included:

- Meeting the government's requests promptly;
- Making foreign-based employees available for interviews;
- Collecting and producing voluminous relevant documents to the government, including documents located outside the United States;
- Making several detailed factual presentations to the government and conducting and producing financial analyses of voluminous transactions; and
- Timely accepting responsibility and reaching a prompt resolution.

Tysers engaged in timely remedial measures, which included, among other things:

- Placing employees involved in the misconduct on paid administrative leave;
- Terminating all business and affiliations with the intermediary company involved in the misconduct; and
- Comprehensively reviewing and enhancing its compliance program, including engaging additional resources with appropriate expertise to assist in evaluating and strengthening its compliance program, making enhancements to the governance and oversight of its compliance program, adding new compliance resources and personnel, updating and enhancing its antibribery and anticorruption policies, enhancing procedures related to onboarding and making payments to third-parties, and enhancing training programs.

In light of these considerations, Tysers' criminal penalty calculated under the U.S. Sentencing Guidelines reflects a 25% reduction off the bottom of the applicable guidelines fine range.

H.W. Wood

Pursuant to its DPA, H.W. Wood agreed, based on the application of the U.S. Sentencing Guidelines, that **the appropriate criminal penalty is $22.5 million and approximately $2.3 million is forfeitable** to the United States. However, due to H.W. Wood's financial condition and demonstrated inability to pay the penalty calculated under the U.S. Sentencing Guidelines, H.W.

Continues on next page

Continued from previous page

Wood and the department agreed, **consistent with the department's inability to pay guidance, that the appropriate criminal penalty is $508,000** and that H.W. Wood is unable to pay the forfeiture amount. The department reached this resolution with H.W. Wood based on a number of factors, including, among others, the nature and seriousness of the offense. H.W. Wood received credit for its cooperation with the department's investigation, which included:

• Meeting the government's requests promptly;

• Endeavoring to make foreign-based employees available for interviews;

• Collecting and producing voluminous relevant documents to the government, including documents located outside the United States;

• Making several detailed factual presentations to the government and conducting and producing financial analyses of voluminous transactions; and

• Timely accepting responsibility and reaching a prompt resolution.

H.W. Wood engaged in timely remedial measures, which included, among other things:

• Terminating an employee involved in the misconduct; and

• Enhancing its compliance program, including creating new compliance positions and compliance control improvements, implementing a process to ensure continuous monitoring and review of third-party relationships, and updating and enhancing its policies and procedures, as well as its compliance training and communications.

In light of these considerations, H.W. Wood's criminal penalty calculated under the U.S. Sentencing Guidelines reflects a 25% reduction off the bottom of the applicable guidelines fine range. [11434]

BRIEFS

Post Acquisition Disclosure Yields Declination

➤ On November 16, 2023, the U.S. Department of Justice (DOJ) issued a letter to **Lifecore Biomedical, Inc.**, formerly known as Landec Corporation, under the agency's Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy. This letter was a "declination with disgorgement," indicating that the DOJ decided not to prosecute Lifecore despite identified misconduct.

The situation involved FCPA violations by Lifecore's former subsidiary, **Yucatan Foods**. It was found that employees and agents of Yucatan Foods had engaged in bribery, specifically paying bribes to Mexican government officials to secure a wastewater discharge permit.

Despite these findings, the DOJ declined to prosecute Lifecore, acknowledging the company's proactive measures. During Lifecore's pre-acquisition due snok, at least one Yucatan officer involved in the misconduct (the "Yucatan Officer") took affirmative steps to conceal the misconduct from Lifecore and its auditor. After Lifecore learned of the misconduct during post-acquisition integration, it initiated an internal investigation that led to voluntary self-disclosure within three month. The company also quickly took steps to rectify the misconduct. [11417]

Binance Sandbagged by Treasury, Justice & CFTC

➤ Binance Holdings Limited the entity that operates the world's largest cryptocurrency exchange, **Binance.com**, pleaded guilty and has agreed to pay over $4 billion to resolve the Justice Department's investigation into violations related to the Bank Secrecy Act (BSA), failure to register as a money transmitting business, and the International Emergency Economic Powers Act (IEEPA)

Binance's founder and CEO Changpeng Zhao, a Canadian national, also pleaded guilty to failing to maintain an effective anti-money laundering (AML) program, in violation of the BSA and has resigned.

Binance's guilty plea is part of coordinated resolutions with the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC) and the U.S. Commodity Futures Trading Commission (CFTC).

"In just the past month, the Justice Department has successfully prosecuted the CEOs of two of the world's largest cryptocurrency exchanges in two separate criminal cases," said **Attorney General Merrick Garland.** "The message here should be clear: using new technology to break the law does not make you a disruptor, it makes you a criminal."

The announcements by Justice, Treasury and the CFTC did not address the outstanding prosecution by the Securities and Exchange Commission. [11433]

Report: Applied Materials Violated Export Laws

➤ Reuters reports semiconductor equipment maker **Applied Materials** is under U.S. criminal investigation for potentially evading export restrictions on China's top chipmaker SMIC.

The largest U.S. semiconductor equipment maker is being probed by the Justice Department for sending equipment to SMIC via South Korea without export licenses, the report said. Hundreds of millions of dollars of equipment is beleived to be involved.

Santa Clara, Cal.-based Applied Materials said it first disclosed in Oct. 2022 that it had received a subpoena from the U.S. Attorney's Office in Massachusetts for information on certain China customer shipments."The company is cooperating with the government and remains committed to compliance and global laws, including export controls and trade regulations," it said in a statement. [11436]

Texans Convicted in Iran-China Oil Scheme

➤ Two Texas men were convicted Nov. 15, 2023 on charges of attempting to violate the International Emergency Economic Powers Act (IEEPA), conspiracy to violate IEEPA, and conspiracy to commit money laundering in connection with their attempt to transact in sanctioned Iranian petroleum and launder the proceeds.

In 2019 and early 2020, **Zhenyu "Bill" Wang** and **Daniel Ray Lane** engaged in a conspiracy to purchase petroleum from Iran, in violation of economic sanctions imposed by the U.S. under IEEPA. They then planned to mask the origins of the petroleum and sell it to a refinery in China.

The defendants also attempted to conceal their transactions by obtaining foreign passports, engaging in sham contractual agreements, and conspiring to launder the proceeds of the sale through shell entities and offshore financial accounts. For example, Lane offered to use the mineral rights that his company sold to launder proceeds for the Iranian sellers. In addition, Wang arranged for bribe payments to be paid the Chinese officials and bankers.

Wang and Lane, as well as three co-conspirators, were originally charged by complaint in Feb. 2020. They face each a maximum penalty of 45 years in prison: five years for conspiracy to violate IEEPA and 20 years each for attempting to violate the IEEPA and conspiracy to commit money laundering counts. [11435]

Payments Firm Settles for Peanuts

➤ OFAC settled with **daVinci Payments** Nov. 6 for its violations of sanctions with Crimea, Cuba, Iran and Syria for $16.64 per violation. daVinci, which offers rewards cards for various clients, was found to have permitted users in sanctioned countries to receive rewards despite sanctions.

The company "agreed to remit $206,213 to settle its potential civil liability for 12,391 apparent violations" in the four countries, according to a Treasury press release.

"The settlement amount reflects OFAC's determination that daVinci's conduct was non-egregious and was voluntarily self-disclosed," the release said.

Fellow rewards processor **Tango Card** settled similar charges in October 2022. In that case, potential penalties in excess of $9 billion were reduced to $116,000. [11386]

Server Sales Earn 18-Month Sentence

➤ A California man was sentenced to 18 months in federal prison for conspiring to procure and illegally ship high-end computer servers from the U.S. to Iran, in violation of the International Emergency Powers Act (IEEPA) and U.S. sanctions against Iran.

Johnny Paul Tourino, 69, of Dana Point, was sentenced Dec. 8, as well as fined $20,000. Tourino agreed to forfeit approximately $2 million in seized funds.

On March 3, Tourino pleaded guilty to one count of conspiracy to violate IEEPA, which controls and restricts the export of certain goods from the U.S. to foreign nations, as well as U.S. sanctions against Iran. [11498]

Hoosier Brothers Built Machine guns for ISIS

➤ The elder of two Indiana brothers, **Moyad Dannon,** was sentenced to 200 months in federal prison followed by a lifetime of supervised release, after pleading guilty to attempting to provide material support or resources, namely, firearms, to a designated foreign terrorist organization. Moyad's brother, **Mahde Dannon**, was sentenced to 20 years in prison in October 2021, after pleading guilty to the same charges. At the time of their arrests (2018) the men were aged 21 and 20, respectively.

In 2018 the brothers sold a number of illegally obtained firearms to an FBI Informant. They also manufactured untraceable fully automatic "ghost guns" by purchasing firearms parts online and assembling those parts into rifles, and selling those weapons to an undercover agent and the informant, believing tithe weapons would be shipped to the Middle East, to ISIS. [11514]

More Industry Input on Export Controls

Commerce Secretary Gina Raimondo announced plans to create an Export Control Advisory Panel "to help us get our export controls to be more effective by having a continuous engagement with industry." The announcement was included in her remarks to the Fall meeting of the President's Export Council (PEC) Nov. 29, 2023, which included a recap of AI initiatives and the announcement of a mission to the ASEAN region in March.

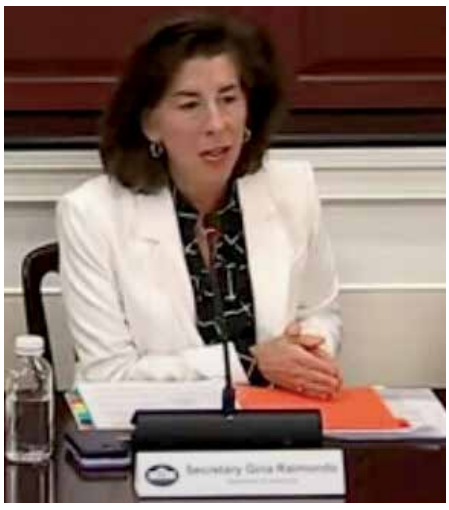
"Three quick things from me which are, I think, responsive to what I said I would do and what you asked me to do at the first meeting. We had a first meeting, we had a lunch. I talked to each of you, you gave me some feedback.

U.S. Artificial Intelligence Safety Institute (USAISI)

"So first you said that we should get more involved with artificial intelligence, and we started that. The Commerce Department is leading the administration's work on artificial intelligence. About three weeks ago in the UK, we launched from the Commerce Department the AI Safety Institute. The concept here is that you can only harness the benefit of AI if you first kind of keep a lid on the risk. And the risks are significant and growing, especially national security risks.

"We are standing up in the Commerce Department a permanent new institute of scientists, academicians, engineers, people from industry to come up with guardrails and safety protocols so that we develop AI in a way that is safe.

"You're going to be using in every one of your businesses 10 times more than you already are. And so we're going to make sure that the work we are doing at Commerce is fully integrated with what's happening at the PEC.



Secretary Gina Raimondo

Reviving the President's Export Council Subcommittee on Export Administration (PECSEA)

"Secondly, how do we get the PEC more involved with our technology efforts and our export controls? I'm very pleased to announce now that we are reconstituting* what's called PECSEA, which Lisa [Disbrow] will chair. We're going to put out a notice of solicitation for members. We're looking for senior executives and your senior product people. We need the people at the cutting edge of the technology, so government works hand in glove with companies we need to control.

"We need to find that magic line of what we control. We don't want to over control, because then we deny you as companies revenue that you need to grow. But we can't under control because then our adversaries get access to our cutting edge technology and use it against us.

"The PECSEA is in line with the recommendation you gave us last time. We're going to gather insights from the new committee to help us

get our export controls to be more effective by having a continuous engagement with industry.

"I just want to like say on this: it's not enough to say we get a piece of intelligence that some equipment has to be controlled, and then we call industry feverishly. We want to have a constant, continuous dialogue with industry so it can be more strategic.

**Begun in 1976, the PECSEA was discontinued during the Trump Administration.*

March Mission to Philippines and Thailand

"Last time at this meeting we we talked about doing a a mission together to the region as APEC and so I'm announcing we're going to do a PEC mission to the Indo Pacific — Philippines and Thailand. Tentatively now is the week of March 11th, we've already started the planning. So I don't know, I feel like that's pretty good progress in only two meetings." [11446]

Quint-Seal: 'Know Your Cargo' Bulletin

FIVE FEDERAL TRADE ENFORCEMENT AGENCIES issued a "Know Your Cargo" announcement to industry Monday, describing best practices for shippers to comply with the current enforcement regime.

The Department of Justice, Commerce's Bureau of Industry and Security (BIS), Department of Homeland Security's Homeland Security Investigations, State's Directorate of Defense Trade Controls (DDTC), and Treasury's Office of Foreign Assets Control (OFAC) issued the joint compliance note, advising entities in maritime and transportation industries to implement compliance measures against illicit practices, particularly in high-risk areas and cargo types.

ADOBE STOCK

Common Ruses

These illicit practices include:

• **Manipulating Location or Identification Data:** This involves disabling or falsifying Automatic Identification System (AIS) data to hide a vessel's location or movement, and altering vessel identifiers like names and IMO numbers. Use of commercial satellite imagery can help in monitoring vessels.

• **Falsifying Cargo and Vessel Documents:** Entities may use forged documents like bills of lading and certificates of origin to disguise cargo's origin or destination.

• **Ship-to-Ship Transfers:** Often legitimate, but sometimes used illicitly to conceal cargo's origin or destination, especially when conducted at night or in high-risk areas.

• **Voyage Irregularities and Abnormal Shipping Routes:** Illicit traders may use indirect routing or unscheduled detours to disguise cargo's destination or origin.

• **Frequent Registration Changes:** Vessels may repeatedly re-register under different flags to evade regulations, a practice known as "flag hopping."

• **Complex Ownership or Management Structures:** Illicit actors may use shell companies or obscure ownership structures to hide the true owner of cargo or end user.

Compliance Tips

The note goes on to describe steps that maritime and other transportation industries can take to enhance compliance controls, particularly in high-risk areas or when encountering anomalous behaviors indicative of deceptive shipping. Key compliance practices include:

Continues on next page

Continued from previous page

• **Institutionalizing Sanctions and Export Control Compliance Programs:** Develop and adhere to risk-based compliance policies and procedures. Encourage industry partners to have similar compliance policies. Utilize U.S. government resources for program development.

• **Establishing Location Monitoring Best Practices and Contractual Requirements:** Conduct due diligence on the location history of vessels, vehicles, and aircraft. Encourage continuous broadcasting of tracking data and investigate any data manipulation. Include contractual language to prohibit dealings restricted under U.S. laws.

• **Knowing Your Customer:** Perform risk-based due diligence on counterparties, including screening against government lists like the U.S. Government's Consolidated Screening List.

• **Exercising Supply Chain Due Diligence:** Ensure supply chain participants are compliant with U.S. sanctions and export control laws. This includes verifying shipping documentation and licenses, and ensuring cargo reaches its intended destination.

• **Industry Information Sharing:** Foster industry-wide awareness by sharing relevant information within and across industries and supply chains.

Entities are advised to report any detected red flags to U.S. authorities, aiding in the protection of business interests, international commerce, and national security against illicit activities. **BIS anticipates updating this guidance in the near future.** [11500]

BIS

License Rules Loosen for Allies

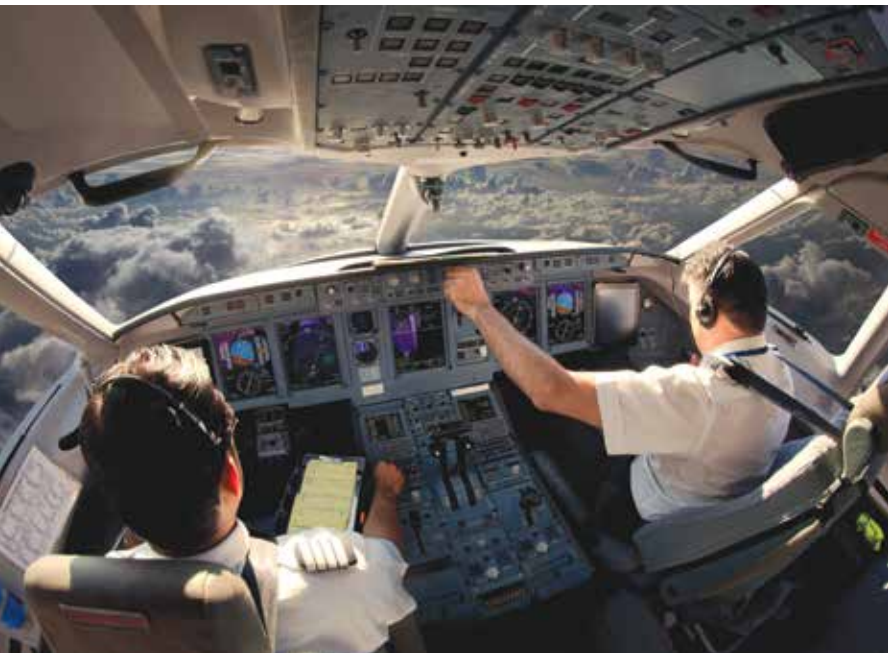
COMMERCE DEPARTMENT'S Bureau of Industry and Security (BIS) has released three rules as part of a broad effort to ease several categories of export licensing requirements and expand the availability of export license exceptions for key allied and partner countries, as well as for members of certain multilateral export control regimes.

"These rules will more accurately reflect the current national security and foreign policy posture of the United States Government," **said Under Secretary of Commerce for Industry and Security Alan Estevez**. "They will create a stronger environment to facilitate cooperation by reducing the licensing burden for items destined to our closest allies and partners."

"These regulations are a result of our assessment of feedback from our allies and partners to harmonize controls and reduce licensing burdens," **said Assistant Secretary of Commerce for Export Administration Thea D. Rozman Kendler**. "They reflect the deep trust and close export control coordination that the United States has fostered with allies and partners for years, which has redoubled in response to Russia's aggression against Ukraine."

Certain components used for the production of civil manned aircraft will now be eligible for an EAR license.

PETROVALEXEY / ADOBESTOCK



Pathogens & Toxins

The first rule changes licensing requirements for certain Australia Group (AG)-controlled pathogens and toxins (and their related technologies) so that no license is required to AG countries, unless the item is also subject to Chemical Weapons Convention controls. It also removes crime control licensing requirements for Austria, Finland, Ireland, Liechtenstein, South Ko-

rea, Sweden, and Switzerland. These countries are in the Global Export Controls Coalition (GECC) (countries listed in supplement 3 to part 746 of the Export Administration Regulations (EAR)) and maintain a commitment to protecting human rights.

Missile Technology Exceptions

The second rule expands license exception eligibility to additional countries for certain missile technology items excluding any countries of concern for missile technology reasons or that are subject to a U.S. arms embargo (i.e., countries specified in Country Groups D:4 or D:5). For example, certain components used in or for the "production" of civil manned aircraft will now be eligible for an EAR license exception to countries that are in both Country Group A:2 and the GECC. The second rule also updates list-based controls to align with recent Missile Technology Control Regime (MTCR) control list changes.

License Exception Strategic Trade Authorization (STA)

The third rule seeks public comment on ways to facilitate use of License Exception Strategic Trade Authorization (STA), including by clarifying which items are eligible for STA to certain destinations, and proposing a number of changes intended to increase the usage of STA and reduce the burden on exporters, reexporters, and transferors, while at the same time still ensuring that U.S. national security and foreign policy interests are protected for items authored under STA.

For example, the rule proposes to allow National Security (NS)-only reason for control items received under STA to be reexported between or among countries that are in both A:5 and the GECC with authorization from the competent authorities of those countries under license exception Additional Permissive Reexports (APR). [11484]

BRIEFS

BIS

Update Conference Rescheduled to March

➤ The Bureau of Industry and Security (BIS) has rescheduled their annual **Update Conference on Export Controls and Policy** to March 27-29, 2024.

BIS anticipates that the planned agenda for the rescheduled conference, while subject to change will include sessions on the following:

- Semiconductors I: Semiconductor Tools
- Semiconductors II: Advanced Computing
- Regulatory Updates
- U.S. Persons Activities
- Foreign Direct Product Rules Overview
- Anatomy of a Disruptive Technology Strike Force Investigation
- Interagency Update
- Export Control Officers Abroad
- Human Rights Due Diligence
- DDTC Updates (invited)
- Census Updates (invited)
- The Entity List ERC
- BIS Data Analysis
- China Brief
- Russia Brief
- International Cooperation and Export Controls
- License Application Tips

The venue for the rescheduled conference remains the Marriott Marquis hotel in Washington, D.C.

BIS

Website Overhaul

➤ The Bureau of Industry and Security released a beta version of its **new website** in December, making changes to functionality and user experience. The sleek new site, accessible from the old website, is more visually appealing and features more user-friendly navigation.

The News & Updates feature on the new site offers many filters to target searches of the Bureau's news archives.

However, some information was not available on the beta site — notably, the E-FOIA option was missing. (The E-FOIA function on the old version of the website was also no longer operational.)

In streamlining its visual display, the new site seems to lack much of its predecessor's information on regulations and policy guidance. Much of the data hosted on the old site is gone, too.

The site disclaims that it is "an early, in-progress version that incorporates new tools to access and use BIS regulations. Results from this beta site may be inaccurate or incomplete and should not be relied upon for compliance with the EAR."

OIG

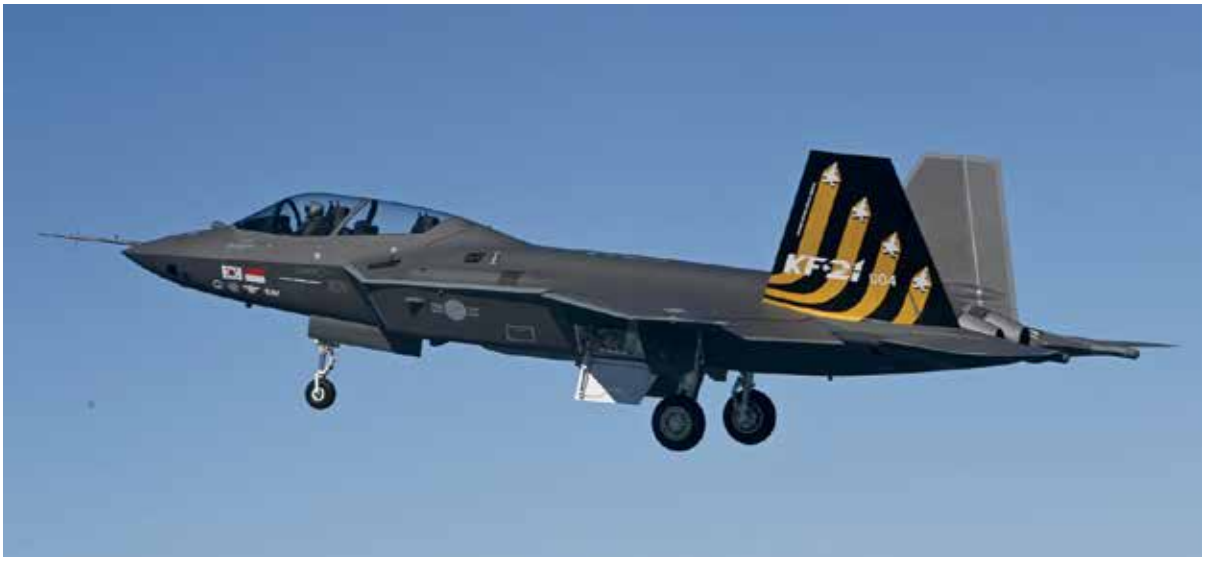
End-Use Monitor Report

➤ The Office of Inspector General (OIG) for the Department of State has released a redacted report detailing its review of **end-use monitoring (EUM) for U.S. security assistance in Ukraine.** This follows the U.S. commitment of approximately $30 billion in aid since Russia's invasion in February 2022.

Findings indicate that Embassy Kyiv conducted limited in-person EUM ac-

Continues on next page

BRIEFS



KOREA AEROSPACE INDUSTRIES

The Department of State temporarily modified the United States Munitions List (USML) Category VIII to accommodate the Korean production of their KF-21 Stealth Fighter.

Continued from previous page

tivities, supplemented by secondary procedures involving Ukrainian government assistance. No misuse of equipment was identified, and commitments from recipients remained unchanged post-invasion.

However, challenges like security restrictions and ad-hoc reporting of battlefield losses were noted.

The redacted report, including the Department's responses and OIG's recommendations, contains information that is Sensitive But Unclassified (SBU) and is not available for public viewing. [11389]

EU

Primer on Dual-Use and Cyber Surveillance

➤ The European Union released an overview of current EU export controls of dual-use items in general and cyber-surveillance items, and what the approach is in countries such as the U.S., the UK and Japan. It explains the impact of the sanctions against Russia on the export of dual-use items and the use of cyber-surveillance in the conflict in the Ukraine.

The Dual-use Regulation 2021/821 has broadened the scope of export controls and defines a new category of dual-use items, namely 'cyber-surveillance items' which is incorporated in the list of dual-use items in Annex I of the Regulation.

Further-more, the Regulation introduces a catch-all clause which makes the export of cyber-surveillance items not listed in Annex I subject to export authorization when intended for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law.

Regarding the sanctions against Russia, the EU had published 11 sanctions packages by mid-November 2023, including the prohibition of direct or indirect export to Russia of dual-use items listed in Annex I of the EU Dual-use Regulation. In addition, technologically advanced items as listed in Annex VII to the sanctions Regulation 833/2014 are also prohibited for export to Russia. [11438]

DDTC

Temporary USML Mod for Korea Fighter

➤ The Department of State temporarily modified the United States Munitions List (USML) Category VIII to accommodate the **Korean production of their KF-21 Stealth Fighter**.

The Department assessed that this temporary modification does not change the export jurisdiction or classification of any existing commodities, as it only prevents the possibility of future release from paragraph (h)(1) due to use in the KF–21, which has not yet entered into production. Therefore, when the KF–21 enters production, any paragraph (h)(1) commodities authorized for export for this purpose will retain their current export classification described in paragraph (h)(1). [11474]

Russia Sanction Efforts Continue

Treasury's Office of Foreign Assets Control (OFAC) and the State Department announced sanctions on over 100 entities and individuals including those engaged in sanctions evasion in numerous third countries complicit in furthering Russia's ability to wage its war against Ukraine, and responsible for bolstering Russia's future energy production and export capacity.

Third-Country Actors

The Dec. 11, 2023 action highlights Russia's utilization of Türkiye, the United Arab Emirates (UAE), and the People's Republic of China (PRC), as well as the use of complex transnational networks and third-country cut-outs, to acquire much-needed technology and equipment for its war economy.

OFAC is designating a network of four entities and nine individuals based in the PRC, the Russian Federation, Hong Kong, and Pakistan involved in the facilitation and procurement of Chinese-manufactured weapons and technologies to Russia.

Chinese arms trader Hi Xiaoxun and affiliated entities structured deals circumventing U.S. sanctions and Chinese controls on the export of military-related materials, including for conventional weapons and electronic components with Russian customers for ammunition, loitering munitions, and semiconductor microchip manufacturing equipment.

Seven Turkish firms were cited for shipments of common high priority items to Russia-based manufacturers, including shipments of ball or roller bearings and microelectronics.

Continues on next page

Moscow International Business and Financial Center
ADOBE STOCK

OFAC

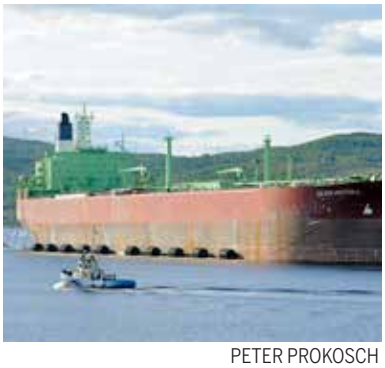
Oil Price Cap Enforcement

EARLIER, OFAC SANCTIONED THREE entities and blocked three vessels that used Price Cap Coalition services while carrying Russian crude oil priced above $70 per barrel after the price cap took effect.

In a related action, OFAC is issuing Russia-related General License 78, "Authorizing Limited Safety and Environmental Transactions Involving Certain Persons or Vessels Blocked on December 1, 2023."

The U.S. is part of an international coalition of countries (the Price Cap Coalition), including the G7, the European Union, and Australia, that have agreed to prohibit the import of crude oil and petroleum products of Russian Federation origin.

These countries, have also agreed to restrict a broad range of services related to the maritime transport of crude oil and petroleum products of Russian Federation origin — unless that oil is bought and sold at or below the specific price caps established by the Coalition or is authorized by a license. [11451]



PETER PROKOSCH

Continued from previous page

The UAE has emerged as a vital transshipment point for aircraft spares and equipment. OFAC cited **eight Emirati** aviation parts and forwarding firms for illicit shipments.

A further four Chinese were cited for trade including satellite imagery used to support Russian operations in Ukraine, microelectronics, and machine tools.

Other actors and entities were cited in **South Korea, Switzerland, Singapore, Kyrgyz Republic, Maldives** and **Tajikistan**.

Russian Entities

Additional Russian companies were named in the recent action, covering a wide swath of Russian industry, from batteries and bearings to aircraft components, microelectronics, and the developer responsible for the Moscow International Business Center, home to seven of Europe's ten-highest skyscrapers.

The actions included three companies developing the Ust-Luga liquefied natural gas (LNG) terminal, a facility at a Baltic seaport in northwest Russia to be operated by **Gazprom** and **RusGazDobycha**, as well as mining tycoon **Vladislav Sviblov** and several affliliated companies.

OFAC also designated four Russian Financial Institutions involved in banking and asset management, including a prominent banker for western companies looking to exit Russia. [11507]

Belarus Actions

OFAC DESIGNATED 11 ENTITIES and seven individuals December 5 to increase the pressure on **Alyaksandr Lukashenka**'s regime for its suppression of Belarus's democratic civil society, financial enrichment of the Lukashenka family, and complicity in Russia's war against Ukraine.

Included in the sanctions are the Secretary General of the Belarus Red Cross, **Dzmitry Shautsou**. Russia's federal government and Belarus' regime have been working together to coordinate and fund the movement of children from Ukraine to Belarus. Both Ukraine and the Belarusian democratic opposition have labelled the transfers unlawful deportations.

On Oct. 4, 2023, IFRC called for Shautsou's removal, and on Dec. 1, 2023, IFRC suspended the membership of the Belarus Red Cross Society for non-compliance with this order due to their refusal to remove him from his position.

Lukashenka crony **Aliaksandr Shakutsin** and his form **Amkodor** have enjoyed a favored position in the supply of western construction equipment into Russia, as well as the development and production of attack drones and artillery fire systems.

The new sanctions also include cement, logging, pulp & paper interests, as well as **Beltamozhservice**, a state-owned Belarusian logistics provider that operates under Belarus's State Customs Committee.

Also sanctioned is Tabak Invest, the only private producer of tobacco in Belarus. Its principals have been "heavily involved in an elaborate cigarette smuggling scheme into Russia," according to the Treasury statement.

Other entities included in the sanctions action are involved in the optics and optoelectronics sectors, as well as radar and microelectronics manufacturers. [11479]

Alert on Russian Gold

BRITAIN'S NATIONAL CRIME AGENCY has issued an alert warning that Russia is using gold as a means to undermine the impact of the UK sanctions regime.

Gold is a significant income stream for Russia's war effort — one of the highest by value after oil and gas, and worth £12.6 billion to the Russian economy in 2021. Given the importance of the UK to the gold market, the NCA is warning of deliberate attempts are being made to launder sanctioned gold to mask its origin so that it can be hidden in supply chains and sold in the UK and around the world.

Gold exported from Russia since 21 July 2022 is increasingly being shipped to countries that do not apply sanctions on Russian gold. Once melted down and recast or refined, the origin of gold cannot be determined by examination, as any hallmarks are lost. Imports of mined gold can also be easily disguised. By masking the origin, new Russian gold can then be sold on to another country who may be unaware of the true origin. [11383]

ADOBE STOCK

Gold smelting

Venezuela Sanction Update

TREASURY'S OFFICE OF FOREIGN Assets Control (OFAC) is issuing Venezuela-related General License 8M, "Authorizing Transactions Involving Petróleos de Venezuela, S.A. (PdVSA) Necessary for the Limited Maintenance of Essential Operations in Venezuela or the Wind Down of Operations in Venezuela for Certain Entities," and Venezuela-related General License 45A, "Authorizing Certain Transactions Involving Consorcio Venezolano de Industrias Aeronáuticas y Servicios Aéreos, S.A."

Additionally, OFAC is publishing an updated, related document "Frequently Asked Questions Related to the Suspension of Certain U.S. Sanctions with Respect to Venezuela on October 18, 2023."

The U.S. government suspended certain sanctions measures on **Venezuela's oil and gas sector operations; the gold sector of the Venezuelan economy**; and U.S. person purchases in the secondary market of certain **Venezuela sovereign bonds and equity**. The U.S. government has suspended these sanctions measures "in response to recent concrete steps toward a democratic solution in Venezuela," according to the Treasury.

The authorization in GL 44 suspends Venezuela-related sanctions applicable to most oil and gas sector operations in Venezuela, including the sale of oil and gas from Venezuela to the U.S. and other jurisdictions, as well as the payment of taxes, royalties, costs, fees, dividends, and profits related to oil and gas sector operations or transactions involving PdVSA.

While GL 44 provides broad relief to oil and gas sector operations in Venezuela, several key prohibitions remain in place, related to banking services and payments, Russian investment in Venezuelan oil facilities, and virtual currencies. Venezuela-related sanctions suspended on Oct. 18, 2023 do not affect the U.S. government's posture on litigation brought by creditors seeking to attach assets of the Government of Venezuela in the U.S..

Renewal of GL 44 is subject to the representatives of Maduro following through with their commitments and taking concrete steps toward a democratic election by the end of 2024.

Gold Sector

OFAC also issued General License (GL) 43 on Oct. 18, 2023, which authorizes all transactions involving CVG Compania General de Mineria de Venezuela CA (Minerven) — the only entity designated by OFAC for operating in the gold sector of the Venezuelan economy — that are prohibited by the Venezuela Sanctions Regulations. [11413]

GAZA & WEST BANK

Compliant Humanitarian Assistance

OFAC ISSUED OFAC Compliance Communiqué: Guidance for the Provision of Humanitarian Assistance to the Palestinian People in response to questions from the NGO community and the general public on how to provide humanitarian assistance while complying with OFAC sanctions.

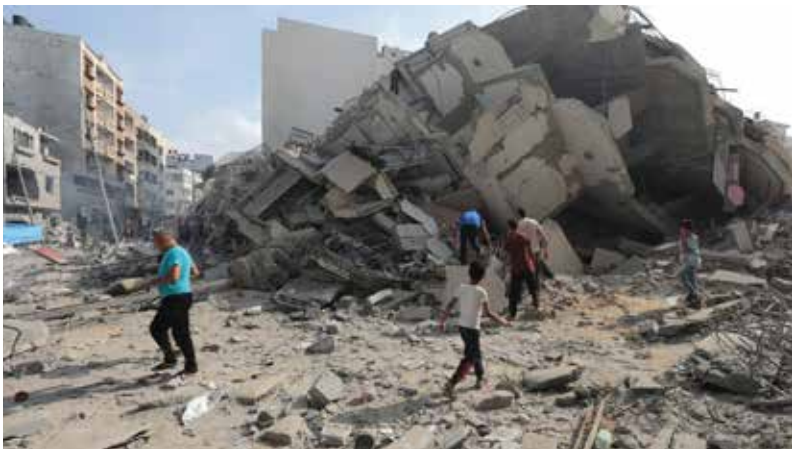
Neither Gaza nor the West Bank are subject to jurisdiction-based sanctions or an embargo by OFAC. Further, OFAC authorizes limited transactions with blocked persons to the extent such dealings are ordinarily incident and necessary to certain humanitarian activity,

Sections 594.520 and 597.516 ("the NGO general licenses") authorize all transactions that may otherwise be prohibited in support of certain NGO non-commercial, humanitarian-related activities, subject to certain conditions.

For example, an NGO may provide life-saving medical assistance to civilians in Gaza at a hospital staffed or occupied by Hamas

Since the U.S. does not maintain jurisdiction-based sanctions or an embargo on Gaza or the West Bank, the provision of food, other agricultural commodities, medicine, and medical devices is generally not prohibited.

U.S. government and international organizations are approved under the "USG General Licenses" and "IO General Licenses." [11412]



Palestinians inspect the ruins of Aklouk Tower destroyed in Israeli airstrikes in Gaza City on October 8, 2023.
WIKIMEDIA COMMONS

BRIEFS

Beneficial Ownership Deadline Extended

➤ The Financial Crimes Enforcement Network (FinCEN) issued a final rule Nov 29 that extends the deadline for certain reporting companies to file their **initial beneficial ownership information (BOI) reports** with FinCEN.

Reporting companies created or registered in 2024 will have 90 calendar days from the date of receiving actual or public notice of their creation or registration becoming effective to file their initial reports. FinCEN will not accept BOI reports from reporting companies until January 1, 2024 — no reports should be submitted to FinCEN before that date. [11447]

IRAN

More Military Entities

➤ Treasury's Office of Foreign Assets Control (OFAC) sanctioned over 20 individuals and entities for their involvement in financial facilitation networks for the benefit of **Iran's Ministry of Defense and Armed Forces Logistics (MODAFL) and Iranian Armed Forces General Staff (AFGS), and the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF).**

MODAFL and the AFGS sell commodities through a network of front companies both inside Iran and abroad, including Sepehr Energy. Sepehr Energy uses companies in Hong Kong and the United Arab Emirates to sell billions of dollars' worth of commodities to customers in Europe and East Asia. [11452]

VENEZUELA

Aircraft Parts

➤ The ERC determined to add **Aerofalcon S.L.**, under the destination of Spain; **Novax Group S.A.,** under the destinations of Costa Rica, Ecuador, Panama, Venezuela, and Russia; and **Zero Waste Global SA**, under the destinations of Panama and Venezuela, to the Entity List.

These entities were used by their principals to circumvent U.S. sanctions, supplying the representatives of Nicolás Maduro

BRIEFS

in Venezuela with U.S. origin aircraft parts.

This circumvention was conducted by, among other efforts, concealing the true end user and end destination of the exports using misrepresentations and fraudulent documents, including the filing of false Electronic Export Information. [11406]

INDIA

Chip Sales to Russia

➤ BIS also determined to add **Si2 Microsystems Private Limited**, under the destination of India, to the Entity List for providing support to Russia's military and/or defense industrial base.

Specifically, this entity supplied Russian consignees connected to the Russian defense sector with U.S.-origin integrated circuits after March 1, 2023.

These integrated circuits are classified under Harmonized Tariff System (HTS)-6 codes 854231, 854232, 854233, and/or 854239. These HTS-6 codes are identified under supplement no. 4 to part 746 (Russian and Belarusian Industry Sector Sanctions Pursuant to § 746.5(a)(1)(ii)).

All U.S.-origin items classified under these HTS-6 codes have been controlled for export and reexport and transfer within Russia since Sept. 15, 2022. Such U.S.-origin items require a license under § 746.5(a)(1)(ii) of the EAR when destined to Russia or Belarus. [11406]

DPRK

Satellite Launch & Cyber Team Cited

➤ In coordination with foreign partners, OFAC sanctioned eight foreign-based Democratic People's Republic of Korea's (DPRK) agents that facilitate sanctions evasion, including revenue generation and missile-related technology procurement that support the DPRK's weapons of mass destruction (WMD) programs.

U.S. and UN-designated **Green Pine** is responsible for approximately half of DPRK arms and related materiel exports. The Reconnaissance General Bureau (RGB)-controlled Green Pine specializes in the production of maritime military craft and armaments and has provided both technical assistance and weapons to Iranian defense-related firms.

Additionally, OFAC sanctioned cyber espionage group **Kimsuky** for gathering intelligence to support the DPRK's strategic objectives.

Kimsuky primarily uses spearphishing to target individuals employed by government, research centers, think tanks, academic institutions, and news media organizations, including entities in Europe, Japan, Russia, South Korea, and the U.S. [11453]

AFGHANISTAN

Former Allies Stole Millions

➤ The U.S. Treasury on December 11 slapped sanctions on a former Afghan official, his son, and related entities, accusing them of misappropriating millions of dollars of funds provided by U.S. government contracts.

The sanctions statement cited former Afghan parliament speaker **Mir Rahman Rahmani** and his son **Ajmal Rahmani**.

"Through their Afghan companies, the Rahmanis perpetrated a complex procurement corruption scheme resulting in the misappropriation of millions of dollars from U.S. Government-funded contracts that supported Afghan security forces," it said, adding that other family members were also designated.

The Sanction action included 21 German companies, eight in Cyprus, six in the U.A.E. and others in Austria, The Netherlands and Bulgaria. [11506]

NICARAGUA

President and Family Targeted

➤ The Biden Administration renewed the Trump-era restrictions on travel and property ownership by **President Daniel Ortega** and his cadre November 17, stating "the situation in Nicaragua continues to pose an unusual and extraordinary threat to the national security and foreign policy of the United States…For this reason, I am continuing for 1 year the national emergency declared in Executive Order 13851 with respect to the situation in Nicaragua. [11416]

GUATEMALA

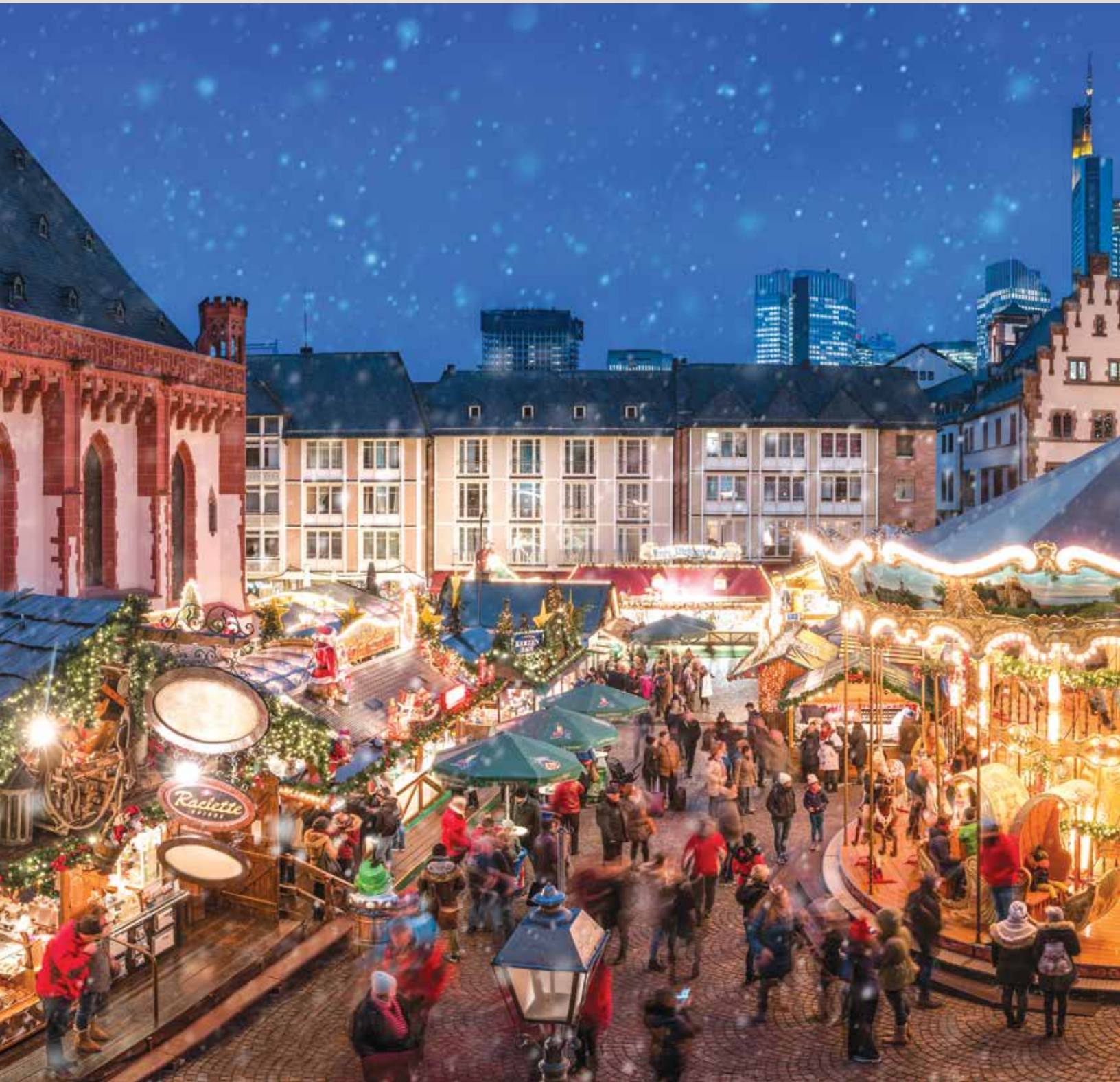
Senior Official Corrupt

➤ OFAC) sanctioned **Luis Miguel Martinez Morales** for his role in corruption in Guatemala wherein he engaged in widespread bribery schemes, including schemes related to government contracts.

Martinez is the former head of the now-defunct Centro de Gobiernoa powerful quasi-cabinet level agency created by Guatemalan President Alejandro Giammattei at the start of his administration.

President Giammattei was forced to shut down the Centro de Gobierno in December 2020 following backlash to Martinez' rising power in the government. [11467]

To read the complete article, please click on the blue number at the end of the story, or go to exportprac.com and search for the number.


Raclette