February 2023 | Vol. 37, No. 2

EP THE EXPORT PRACTITIONER™

IN THIS ISSUE:

- Self Disclosure Incentives Sweetened
- FinCEN – Europol Collaboration
- NASA-USRA Licensing Lapse
- Xinjiang Auto Parts Focus
- DDTC & BIS Updates

Red Flags and End Use Checks

Enforcement: The Export Control Officer's Perspective

MASTERING EXPORT COMPLIANCE

NEWLY UPDATED!

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

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

Mastering Export Compliance covers:

- Overview of Export Controls
- Penalties for Non-Compliance
- EAR and ITAR
- Red Flags for Exporters
- The Role of Federal Agencies
- And more!

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

Contact Frank today at 301-460-3060 or info@tradecompliancegroup.com.

Also available!

Mastering Import Compliance
Mastering Exports to China
Mastering Deemed Exports

THE EXPORT PRACTITIONER™

FEBRUARY 2023 | VOL. 37, NO. 2

THE VIEW FROM FRANKFURT

Red Flags and End Use Checks

ON THE COVER: Red flags fly over China's Tiananmen Square. (ISTOCK XI JINPING: MIRKO KUZMANOVIC)

The Export Practitioner
www.exportprac.com

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

Published monthly by Gilston-Kalin Communications, LLC.

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

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

ISSN 1087-478K

FEATURE

THE VIEW FROM FRANKFURT

An ECO's Perspective on End-Use Checks and Red Flags

BIS Export Control Officers (ECOs) play a unique and critical role in monitoring the compliance of transactions subject to BIS's Export Administration Regulations (EAR) (15 CFR parts 730-774) outside the United States to prevent and detect illicit diversion to unauthorized end uses, end users, or destinations.

Scot Gonzales, Regional Export Control Officer for Western Europe, BIS-Frankfurt, discussed working with ECOs, best practices and red flags, during the 2023 U.S. Export Control Seminar for Canadian and UK Government, Industry, and University Communities Workshop hosted by the US Department of State the last week of January.

Justitia Brunnen, fountain of justice, Römer square, Frankfurt, Germany.

CREATIVE COMMONS: JORBASA FOTOGRAFIE

BIS export enforcement takes a two pronged approach to enforcement and compliance. Our focus isn't just within the borders of the US, but it's also beyond our borders. Based in the US and spread out between 9 field offices and numerous satellite locations are about 130 federal special agents, with full authority to issue subpoenas for records, investigate criminal and administrative leads, carry firearms and make arrests. These agents are subject matter experts in the area of dual use export controls and work with partner agencies like Homeland Security, FBI and others to present cases to the Department of Justice for prosecution.

ECO's like myself are located in seven locations globally from which we all operate

and maintain a regional presence. There are two teams here in Germany, one in Turkey, one in the UAE, one in Hong Kong, two in China, one in Singapore and one in India. However, there are two additional teams that may go online this year as well globally.

We serve as BIS point person within a region by conducting various activities in support of US export controls. This includes end use checks training events like this one. We advise host government, nation governments and businesses on matters related to US export law and how they coordinate with their local laws. And we facilitate information sharing and support of administrative and criminal cases as needed.

Just a quick overview of what I'm going to cover today. We'll talk about what our mission set is for export control officers, some of my recent observations. I'll talk about the end use check program in general, some of the actions we've taken in response to the Russian invasion. I'll give you a quick case example and we'll talk about red flags.

ECO mission areas are varied. We provide foreign government capacity building. We increase cooperation between our partner governments. We've provided training on export controls and counter proliferation issues to harmonize US controls and laws with partner nation government laws and controls. And we develop and strengthen local export control laws. **All of our mission areas are equally important to BIS and our partners in export control, but it's really the end use checks that make up the majority of the work.**

As an example of capacity building, just in the last year BIS established a direct working relationship with the UK Government and HMRC to allow BIS first direct and use verifications within the United Kingdom. We've also been able to expand into new countries within Europe itself as well, providing for greater cooperation between the US and EU partners and greater accountability into the export of controlled commodities. In the area of private sector industry, we continue to do visits and trainings. Trainings have been for individual companies throughout Europe as well as for specific trade associations and industrial sectors. End use checks are where we ensure that US strategic goods and technology are not landing in the wrong hands after they've left the United States.

It has been an interesting year in Europe. Some of the observations and things that I have observed in in the last year are companies who seem to be unfamiliar with their local strategic trade laws or export control laws. It's interesting to note that although companies generally are leading the push towards export compliance and in fact many are over compliant, there are some companies who just aren't familiar with how their business model complies with or may not comply with various trade laws both within their host government and internationally.

ECOs are experts in the area of dual use export controls and work with partner agencies like Homeland Security, FBI and others to present cases to the Department of Justice for prosecution.

We spend a lot of time providing guidance on how to engage with their host governments and get their business practices aligned with those laws. We also have seen a significant number of discrepancies or generic general entries into data records keeping, not listing actual end users and uses and license applications and in other supporting documents, whether it be a request for an end use statement or even in just some of your transactional documents.

Details related to a transaction and its parties are often some of the most overgeneralized things I've seen in my experience. To ensure the proper vetting by the government officials, as well as to ensure due diligence on the part of the businesses, please list as much as you can about your transaction, especially about the parties to your transactions, the commodity descriptions and their usages.

Due diligence is a mainstay to proper export enforcement. Knowing who your customer is can mean the difference between a successful business transaction and government inquiries from individuals and myself or other export

Continues on next page

Continued from previous page

enforcement entities. And it also could lead to potential national security harms.

I can't stress enough, one of the key things is not having a proper or not having an ICP, an internal compliance program at all. And some of my end use checks within the last year I have literally seen organizations create a compliance program the day before my arrival. And while that's a great starting point, you hate for the idea of government engagement to be the reason that you would create the ICP. Do it ahead of time. Use it. There's nothing better than having that compliance program to creating a successful partnership between the governments and business. So please, please, please consider an ICP.

Also consider the changing rules. For example, between the EU and the US, there have been over a dozen tranches of regulations issued since February of last year targeting Russia and Belarus. In addition, there have been regulations issued against China and several other parties worldwide. Keep up to date the European Commission as well as the US.

Long gone are the days of full-fledged weapons systems being routinely shipped and moved around the world. Today we're concerned with commodities and technologies that have very diverse and legitimate use, but a very nefarious illegal use, whether it be chemicals that are making our everyday plastics and can be used in biochem processes, or whether it be machine tools that are used in automotive manufacturing or potentially in support of weapons systems. The job is much more difficult in this sense. The partnership between industry and governments has never been more critical than it is now because of this diversity.

There continue to be multiple media reportings related to Western origin goods having an impact on the battle space in Ukraine. None of us want to be known as the country or company that is the go to supplier of goods to Russia. This is a partnership that we have to continue to work together to plug those holes that make the media splashes that we all too often have seen.

End use checks, as I said, are my biggest cornerstone for compliance with export controls in in the area. Changes to the US law back in 2018 reinforced BIS's role in extraterritorial compliance with US export control laws. A production of records requirement now is required of all parties to a transaction upon request from a representative of BIS. You would be required to produce records as far back as five years due to the statute of limitations. As a condition of receiving items subject to the EAR, foreign consignees are required to provide information as to what you've done with the goods. Thus the end use monitoring aspect of my job.

End use checks are in fact voluntary, but refusing to participate in one does have potential consequences. And by the way, many of our friends are doing it now. At least three European allies are currently conducting their own end use verifications of their export controlled commodities into the countries of import.

End use checks aren't necessarily a review of particular party to a transaction, they're a verification of the entire transaction from beginning to end. We're verifying the conditions of compliance and even compliance of non licensed items and confirming who the end users are.

The biggest goal is to create that positive relationship with industry. The vast majority of businesses have welcomed our checks as an opportunity to enhance or develop internal compliance programs, or simply ask questions of officials to ensure that they are compliant.

Instead of asking why me, most companies are now asking how can we help? Export control is a partnership with industry rather than the burden that it was years ago. In my 19 years with BIS, I've seen the trend change from where, unfortunately, there were companies

Continues on next page

There continue to be multiple media reportings related to Western origin goods having an impact on the battle space in Ukraine. None of us want to be known as the country or company that is the go to supplier of goods to Russia.

— **SCOT GONZALES,** BIS Export Control Officer

Continued from previous page

that took the approach to factor into their budgets a financial calculation as to paying potential penalties if they were to get caught. That move is shifted to having internal compliance programs where they're partnering with and in fact leading the charge on export control.

Some of the transactional documentation that we spend our time reviewing are the obvious. Transactional documents, airway bills, bills of lading, PO RFQ's for the initiate transactions. We also look at packing lists and licensing applications to make sure that proper modify classifications, proper end users are listed, but we also do the same screening that we would impose upon a company in the form of due diligence. Are these parties anywhere subject to any of our lists? Are they subject to restrictions by other partner countries? We look at documents beyond just the scope of the business documents.

End use checks don't necessarily mean BIS has concerns. There are some tens of thousands of shipments a year, and our checks are in the single thousands as we look at randomly selected transactions involving our most critical technologies. And as I mentioned there is a five year statute of limitations, meaning we can conduct end use checks on track on transactions up to five years from date of export.

There are consequences for less than favorable determinations in a check. From a U.S. government perspective, there are only three options: a check can be deemed reliable for the receipt of US goods. The party can be redeemed as unreliable to receive US goods, or party can be unverified. Where a party can be unverified is the problem where we often may be required to take additional actions.

If we are unable to locate or contact a company, or if the company is unable to confirm the ultimate disposition of its commodities, or unfortunately in some locations where the host government doesn't assist or refuses or blocks us from scheduling the end use checks with the company. That company can be placed on the US Department of Commerce's unverified list.

To give you an idea of how things played out over the last year throughout Western Europe, reliable checks have made-up nearly 91% of my checks. So the vast, vast majority of checks are reliable, compliant companies who will continue to be reliable recipients of of US controlled goods.

An unreliable or unverified party then gets potential placement on an unverified list, which, from a US perspective, as the US parties are doing their due diligence in a transaction, a party to an unverified list will alert the US exporter that we've been unable to establish the bona fides of a particular party, and that some license exceptions may not be available and a license may be required. 2022 was a busy year for the unverified list with 33 parties added.

At the same time the process does allow for removal. Where we've had the ability to eventually go in and establish bona fides or meet with companies, we have had the ability to remove them from the entities or the unverified list. Where the unverified list parties remain on there for a period of time, and continued efforts are unfruitful in getting their bona fides confirmed, the potential does exist for those parties to be nominated to the unverified or to the entities list.

The entities list is the BIS's licensing policy position on particular parties of concern who may be acting contrary to national security or foreign policy of the US. It imposes specific restrictions on licenses that may or may not be granted. It would eliminate licensing conditions and would provide for a licensing process and part case by case review of each individual application. In 2022, the vast, vast majority of our parties that were added to the entities list were Russian entities.

It's important to understand that the entity list is Commerce's feed into the consolidated screening list, combined with States designation list and Treasury's designation list. The consolidated screening list is part of a company's due diligence process to make sure that a party involved in their transaction isn't on a prohibited parties list. And as many of my colleagues have said, thankfully we now have the consolidated screening list which allows for parties to review on their own. It is a list of the parties for which

Continues on next page

Continued from previous page

the United States government remains restrictions on certain exports re exports of transfer of items.

We highly suggest that you check the CSL before responding to RFQ's. Before engaging in projects, before shipping, manufacturing or transfer of any monies, make sure that your party is not a member of the party to the consolidated screening list. Make sure that throughout the process, and if your customer is a long term customer, that you routinely check, as the position of some countries and those companies within that country could change on the entities list.

In response to specifically to Russia's invasion of Ukraine, it has been a busy year for BIS enforcement. We've imposed sweeping export controls on Russia and Belarus, along with the European Union and our partners globally. There's been over a 90% reduction in US exports to Russia in the last year as a result of the invasion.

Specific to our enforcement actions, we've conducted outreach and now over 4,000 entities both in the United States and globally on those new export controls. We've detained receive some 250 shipments valued at over $100 million US. We've identified all almost 200 aircraft that are commercial and privately owned who have flown into Russia or Belarus in likely violation of the ER. And we've issued temporary denial orders against those airlines and those air cargo companies regarding those violations, which is prohibiting parties from being able to service those aircraft, fuel them. Even potentially loading onto them may be a violation of the ER as a result of the TDF.

And as I said previously we've added some 300 plus parties from Russia and Belarus and other countries who continue to provide Russian military and defense industry support to the entities list. My colleagues and I have conducted some 500 and use checks specifically targeting possible Russian diversion globally around in the last year.

But it's not just Russia that is the country of concern that we continue to regulate and find transactions of concern on. This is a recent check of mine where I conducted a post shipment verification on electronic components that were shipped, no license required, from the US to the UK. False information provided by the UK company was listed on the end user statement and provided to the US company as the supplier. the US company believed that all the goods were going into UK for use.

However, that's not how it worked. The company sole customer simply sends the shopping list to the UK company, who then purchases controlled commodities from the US, has them shipped to the UK and simply relabels them and ships them onto Hong Kong. Does this seem right to the normal business party? Do you see any red flags here?

Identifying red flags

Speaking of red flags, we spend a lot of our time identifying potential red flags for companies we engage with. Transshipment red flags involved delivery and planned way out of the destinations or freight forwarding firms who are listed as the products' final destination, or shipping routes to seem normal are serious transshipment red flags that we also be aware of.

Recent examples that I've had within the last year: where IC board manufacturers who all of a sudden get requests for just the parts. We don't need you to build the boards, we just need the parts. Or if you're a sector where you know all of your customers and all of a sudden new customer reaches out willing to pay top dollar, no questions asked for an immediate delivery. Or you've received unsolicited requests for quotes from areas geographically where you haven't even targeted for your business model. These are all actually occurring within Europe last year. All of these are highly important red flags that we would ask you to all pay attention to.

Additional red flag indicators that we look at consistently are inconsistent commodity descriptions. Generic terminology describing the technology, weight and size, and as we all know, value is often undervalued for purposes of customs, but that is one of our main red flags. Unusual routing, asking you to route it through multiple freight forwarders or multiple intermediaries. Technologies and then uses that aren't necessarily suited for the country of destination. And product capabilities inconsistent with the Consignees line of business.

I have a colleague who recently did an end use check on a shipment that constituted an entire Internet backbone. Routers, switches, firewalls, the whole collection that would build an Internet backbone, and when he went and did the check, it was at a woman's clothing store. There was no need for that kind of commodity collection to go to this store. And after the end result of the check, it was determined that they bought for somebody else and shipped it onward to a country of concern.

Vague commodity description,

Continues on next page

Continued from previous page

in addition to the generic wording, generic HS coding and no listing of ECNL or commodity classifications of available are also red flags.

In addition to these red flag indicators, don't forget the money. Taking the same route as the goods themselves is the payment offered in a third currency. For example, is this a transaction between the UK and the US and the money is being paid from a bank in Asia or in Africa and the Middle East? Money is often one of the first red flags that we tend to see.

Unfortunately, we're seeing an evolving threat and tradecraft to diversion to attempts. Within the export control realm, we're seeing entities that are trying to incentivize the relocation of R&D facilities overseas. Joint ventures involving foreign entities that you may not know who the true ownership of those foreign entities may be. Universities are being targeted due to their ties to potential defense contractors. Others are providing marketing services in order to gain access to the company.

Foreign intelligence services of various aspects within the commercial transaction are looking to make gains and not knowing your customer can turn illegitimate companies into transactional partners, which may cause you problems. Know your customer. If there's a concern, reach out for more information. Ask the parties to the transaction. Ask your government. Ask us. We're available, as every one of my colleagues will agree, constantly and always willing to be available.

End-use statements are a good option to lock in the purported end use as well as end user information, which we could then use to help establish whether or not this is a legitimate transaction. However, be aware that there is fraud being perpetrated using end use statements. Within last year I've seen legitimate companies who are seeing their letterhead or their logos being used as forgeries. Swiping them off the Internet? Swiping them off of printed material? Where? Bad actors are taking those logos and hoping that US suppliers, government entities, even simple postal UPS, FedEx delivery services don't catch the subterfuge and unwittingly provide the sought after goods to the wrong addresses.

Before engaging in projects, before shipping, manufacturing or transfer of any monies, make sure that your party is not a member of the consolidated screening list.

CREATIVE COMMONS

And always remember, freight forwarders will never be the end user. So when a freight forwarder is involved, and they're providing the information regarding end use statements, ask for additional information from the end user.

Export controls are joint responsibility with joint benefits. It's the responsibility of the government, but it's also the responsibility of the business community to protect national security. And this growing culture of compliance that we're experiencing within the US and in Europe is protecting company reputations, leveling the playing field to the industries. Creating trade benefits where we're now showing companies are reliable recipients and suppliers and encouraging those business relationships and it prevents them.

It almost eliminates my job by mitigating enforcement activities, and my coworkers in the United States are opening investigations. The less government in their action into a business transaction, the better. Government needs the industry support that we've gotten in the last year to two years and then which includes obviously the facilitating of successful end use checks. We must move forward with this continued partnership of working to control the diversions and working to gather to communicate.

SPEECHES OF NOTE

Assistant Attorney General Kenneth A. Polite Jr. gave a speech at Georgetown University announcing revisions to the Criminal Division's Corporate Enforcement Policy in January.

U.S. DEPARTMENT OF JUSTICE

FCPA

Self-Disclosure Incentives Sweetened

IN AN EFFORT TO ENCOURAGE more voluntary self-disclosure, Justice announced revisions to the Corporate Enforcement Policy, which applies to all corporate criminal matters handled by the Criminal Division, including all FCPA cases nationwide.

These revisions provide specific, additional incentives to companies for voluntary self-disclosures, as well as for cooperation and remediation. The revisions make clear that there will be very different outcomes for companies that do not self-disclose, meaningfully cooperate with our investigations, or remediate.

"This is not a race to the bottom," warned **Assistant Attorney General Kenneth Polite** while announcing the new policy. "A reduction of 50% will not be the new norm; it will be reserved for companies that truly distinguish themselves and demonstrate extraordinary cooperation and remediation."

The Criminal Division is issuing this revised Policy, effective on a prospective basis as of January 2023, which provides, *inter alia*, that when a company has voluntarily self-disclosed misconduct to the Criminal Division, fully cooperated, and timely and appropriately remediated, all in accordance with the standards set forth below, there will be a presumption that the company will receive a declination absent aggravating circumstances involving the seriousness of the offense or the nature of the offender.

Polite announced the revisions to the CEP in a speech at the Georgetown Law Center January 17

"While we continue to utilize our investigative resources and partners to uncover wrongdoing, we could never completely identify and address this area of criminality without corporations — our corporate citizens — coming forward and reporting the conduct of these wrongdoers.

That is what motivated the Criminal Division back in April 2016, when we first announced a voluntary self-disclosure incentive program — the FCPA Pilot Program. To be as transparent as possible, at that time we laid out a roadmap for what companies could expect if they chose to self-disclose misconduct, fully cooperate with our investigation, and timely remediate.

In November 2017, we expanded the pilot program to become the FCPA Corporate Enforcement Policy (CEP), which we subsequently incorporated into the Department's Justice Manual. Since at least 2018, we have applied this policy to all corporate cases prosecuted by the Criminal Division.

Our existing policy provides that, if a company voluntarily self-discloses, fully cooperates, and timely and appropriately remediates, there is a presumption that we will decline to prosecute absent certain aggravating circumstances involving the seriousness of the offense or the nature of the offender. These aggravating circumstances include, but are not limited to, involvement by executive management of the company in the misconduct; a significant profit to the company from the wrongdoing; egregiousness or pervasiveness of the misconduct within the company; or criminal recidivism.

Our existing policy also offers the potential benefit of a presumption of a declination to companies that uncover – during the M&A due diligence process – misconduct by subsidiaries or other entities that they are seeking to acquire, and then self-report that misconduct to the Criminal Division.

And if a company self-discloses, but a criminal resolution is warranted, our existing policy offers 50% off of the low end of the applicable Sentencing Guidelines penalty range.

This policy has demonstrated the Department's commitment to rewarding companies that do the right thing when learning about possible misconduct. **For instance, just last month, we announced that we declined to prosecute a French aerospace company, Safran SA, after it disclosed FCPA violations that it uncovered during post-acquisition due diligence.** The bribe payments to a Chinese consultant that the company uncovered occurred between 1999 and 2015, but the company nonetheless made a full disclosure, fully cooperated, ensured that remediation was complete, and agreed to disgorge the ill-gotten gains of its U.S. subsidiary.

Our corporate resolutions with ABB entities in December 2022 illustrate how the CEP applies to companies that fully cooperate and remediate, even if they did not voluntarily disclose the misconduct. ABB had entered into FCPA resolutions with the Department back in 2004 and in 2010. In the wake of its prior misconduct, ABB implemented a compliance program that detected the FCPA misconduct in South Africa, and the company planned to promptly self-disclose it — it had even scheduled a meeting with the government to do so.

Before the meeting, however, a media report drew public attention to the wrongdoing. But because the company could demonstrate intent and efforts to self-disclose prior to, and without any knowledge of, the media report, the Department weighed both the early detection of the misconduct and the intent to disclose it significantly in ABB's favor. ABB also demonstrated its extensive remediation and cooperation. **Despite ABB's recidivist history and the Department's policy disfavoring successive deferred prosecution agreements, parent company ABB Ltd. was still able to avoid a guilty plea, entering into a deferred prosecution agreement with the Department, with two subsidiaries pleading guilty.** That said, because ABB was a recidivist, we did not give the company the benefit of a reduction from the low-end of the Guidelines range. Instead, to account for the recidivism, the reduction was from the midpoint between the middle and high-end of the Guidelines.

When a company has uncovered criminal misconduct in its operations, the clearest path to avoiding a guilty plea or an indictment is voluntary self-disclosure. It is also the clearest path to the greatest incentives that we offer, such as a declination with disgorgement of profits. And a functioning compliance program with effective detection mechanisms best positions companies to not only identify misconduct in the first instance, but to make the important decision of whether to disclose it.

We fully understand the significance of a company's decision to voluntarily self-disclose and fully cooperate, and the consequences that such a decision brings. These

Continues on next page

Continued from previous page

are complex discussions in boardrooms, and each company and each outside counsel should, of course, choose to do what is in the best interest of the company.

But in providing transparency to the potential incentives, we are underscoring that a corporation that falls short of our expectations does so at its own risk. **Make no mistake - failing to self-report, failing to fully cooperate, failing to remediate, can lead to dire consequences.**

As Exhibit A – I give you the Balfour Beatty Communities military housing fraud plea. There was no voluntary self-disclosure. The company's cooperation was lackluster, merely the bare minimum for credit under the Guidelines and a reduction for acceptance of responsibility. It also failed to conduct appropriate remediation in a timely manner. Therefore, the company did not get any additional reduction of the fine amount under our Corporate Enforcement Policy.

In fact, we determined that the starting point for the fine amount should be between the low end and the mid-point of the applicable U.S. Sentencing Guidelines fine range. Moreover, while the company was not a recidivist, we determined that a guilty plea was warranted due to the seriousness and the pervasiveness of the conduct at multiple bases across military branches. And finally, the company's compliance program was inadequate not only at the time of the offense, but also at the time of the resolution, so we imposed an independent compliance monitor.

As this example illustrates, our default is not a declination; it's not an NPA; and it's not a DPA. We have secured six parent-level corporate guilty pleas during my tenure to date, in cases involving a range of conduct, from foreign bribery and bank fraud to emissions testing fraud and spoofing. We take a nuanced but tough approach, calling it like we see it — and we will continue do so. **Companies are not presumed to qualify for a declination —they must earn it by following our policies.**

Now, in September of last year, the Deputy Attorney General asked all Department components to write voluntary self-disclosure policies, to the extent that they didn't already have them, and "to clarify the benefits of promptly coming forward to self-report, so that chief compliance officers, general counsels, and others can make the case in the boardroom that voluntary self-disclosure is a good business decision."

Although the Division already had such a policy, we took the DAG's call as an opportunity to reassess and strengthen it. Which brings us to today. I am proud to announce the first significant changes to the Criminal Division's CEP since 2017.

As you'll hear, these changes offer companies new, significant, and concrete incentives to self-disclose misconduct. And even in situations where companies do not self-disclose, the revisions to the policy provide incentives for companies to go far above and beyond the bare minimum when they cooperate with our investigations.

CEP Revisions

WE ARE CONSTANTLY EVALUATING whether our policies *and p*ractices result in appropriately vigorous and fair corporate enforcement. With that in mind, I am pleased to announce important revisions to our Corporate Enforcement Policy, which applies to all corporatve criminal matters handled by the Criminal Division, including all FCPA cases nationwide. These revisions provide specific, additional incentives to companies for voluntary self-disclosures, as well as for cooperation and remediation. The revisions make clear that there will be very different outcomes for companies that do not self-disclose, meaningfully cooperate with our investigations, or remediate.

I appreciate that in many situations, companies that have identified potential wrongdoing and are weighing whether to self-disclose that conduct to the Department will be concerned that an aggravating factor may prevent a company from obtaining a declination. And that concern may have

Continues on next page

Continued from previous page

led companies and their outside counsel to conclude, under the prior version of the CEP, that it is more prudent not to disclose the misconduct.

The revised CEP presents another path for companies facing such a choice. A path that incentivizes even more robust compliance on the front-end, to prevent misconduct, and requires even more robust cooperation and remediation on the back-end, if a crime occurs. Namely, even if aggravating circumstances are present, although a company will not qualify for a presumption of a declination, under the revised CEP I am announcing today, prosecutors may nonetheless determine that a declination is the appropriate outcome, if the company can demonstrate that it has met each of the following three factors:

• The voluntary self-disclosure was made immediately upon the company becoming aware of the allegation of misconduct;

• At the time of the misconduct and the disclosure, the company had an effective compliance program and system of internal accounting controls that enabled the identification of the misconduct and led to the company's voluntary self-disclosure; and

• The company provided extraordinary cooperation with the Department's investigation and undertook extraordinary remediation.

Each of these factors is familiar. That is by design. We are requiring companies seeking the possibility of a declination—even in the face of aggravating factors—to take extraordinary measures before, during, and after a Criminal Division investigation to earn such an outcome. This possibility is directed squarely at companies that take compliance and good corporate citizenship seriously.

While some companies may be able to overcome the aggravating factors and receive a declination with disgorgement by meeting these criteria, others will not. But the revised CEP I'm announcing today contains incentives for those companies as well.

If a company voluntarily self-discloses misconduct, fully cooperates, and timely and appropriately remediates, but a criminal

Assistant Attorney General Kenneth A. Polite, Jr. delivers remarks on revisions to the criminal division's corporate enforcement policy.

U.S. DEPARTMENT OF JUSTICE

resolution is still warranted, the Criminal Division:

• will accord, or recommend to a sentencing court, at least 50% and up to a 75% reduction off of the low end of the U.S. Sentencing Guidelines (U.S.S.G.) fine range, except in the case of a criminal recidivist, in which case a reduction of at least 50% and up to 75% will generally not be from the low end of the U.S.S.G. fine range, and prosecutors will have discretion to determine the starting point for the reduction based on the particular facts and circumstances of the case;

• In assessing the appropriate form of the resolution, will generally not require a corporate guilty plea—including for criminal recidivists—absent the presence of particularly egregious or multiple aggravating circumstances, such as those described above, excluding recidivism (i.e., involvement by executive management of the company in the misconduct; a significant profit2 to the company from the misconduct; and egregiousness or pervasiveness of the misconduct within the company); and

• generally will not require appointment of a monitor if a company has, at the time of resolution, demonstrated that it has implemented and tested an effective compliance program and remediated the root cause of the misconduct.

This policy applies to all Criminal Division

Continues on next page

Continued from previous page

corporate resolutions, not only voluntary self-disclosure cases. There will be many instances in which a company will not have voluntarily self-disclosed conduct to the Criminal Division. In such circumstances, the revised CEP provides Criminal Division prosecutors with a greater range of options to distinguish among companies that commit crime.

The revised CEP provides incentives for companies that do not voluntarily self-disclose but still fully cooperate and timely and appropriately remediate. In such a case, the Criminal Division will recommend up to a 50% reduction off of the low end of the Guidelines fine range. That is twice the maximum amount of a reduction available under the prior version of the CEP. In the case of a criminal recidivist, the reduction will likely not be off of the low end of the range. And in all cases, prosecutors will have discretion to determine the specific percentage reduction and starting point in the range based on the particular facts and circumstances.

To be sure, while 50% off the low end of the Guidelines range is the maximum available (absent a voluntary self-disclosure) under the revised CEP, each and every company starts at zero cooperation credit and must earn credit based on the parameters and factors outlined in the CEP. This is not a race to the bottom. A reduction of 50% will not be the new norm; it will be reserved for companies that truly distinguish themselves and demonstrate extraordinary cooperation and remediation. But having a greater range of cooperation and remediation credit available — from 0% to 50%, instead of from 0% to 25%, and using the full spectrum of the Guidelines from which to apply those reductions — will allow our prosecutors to draw greater distinctions among the quality of companies' cooperation and remediation.

Many of you may be curious as to how our prosecutors will distinguish between "extraordinary" and "full" cooperation under the revised policy. We are well aware of the differences between corporations and individuals, of course. But with respect to how we consider cooperation, the lens and framework through which we analyze the level and degree of cooperation aren't so different.

I'll note some concepts — immediacy, consistency, degree, and impact — that apply to cooperation by both individuals and corporations, which will help to inform our approach to assessing what is "extraordinary." To defense counsel, recall your days as a prosecutor. In assessing the quality of a cooperator's assistance, we value: when an individual begins to cooperate immediately, and consistently tells the truth; individuals who allow us to obtain evidence we otherwise couldn't get, like quickly obtaining and imaging their electronic devices, or having recorded conversations; cooperation that produces results, like testifying at a trial or providing information that leads to additional convictions.

These, of course, are just examples in the individual context. In many ways, we know "extraordinary cooperation" when we see it, and the differences between "full" and "extraordinary" cooperation are perhaps more in degree than kind. **To receive credit for extraordinary cooperation, companies must go above and beyond the criteria for full cooperation set in our policies—not just run of the mill, or even gold-standard cooperation, but truly extraordinary.** At the same time, the government will not affirmatively direct a company's internal investigation, if it chooses to do one, and companies are often well positioned to know the steps they can take to best cooperate in a particular given case. And of course, the facts and circumstances of each case will be unique.

The policy is sending an undeniable message: come forward, cooperate, and remediate. We are going to be closely examining how companies discipline bad actors and reward the good ones. Our number one goal in this area – as we have repeatedly emphasized – is individual accountability. And we can hold accountable those who are criminally culpable—no matter their seniority—when companies come forward and cooperate with our investigation.

Failing to take these steps, a company runs the risk of increasing its criminal exposure and monetary penalties. We have already used this approach not only in the Balfour Beatty

Continues on next page

Continued from previous page

Communities case, which I mentioned earlier, but also in cases such as the Bank of Nova Scotia spoofing and the Glencore benchmark manipulation resolutions—where we determined that the appropriate starting point for a Guidelines reduction would be *above* the low-end.

In the Glencore Ltd. case, the company only received a minimal reduction for cooperation and remediation under the CEP because of late and incomplete cooperation and failure to take adequate, timely disciplinary measures with respect to certain personnel involved in, or aware of, the criminal conduct—which was pervasive. And in the Bank of Nova Scotia case, we determined that a fine at the top of the applicable Guidelines range was appropriate because instead of remediating, the company's compliance function contributed to the misconduct.

To all assembled, and especially our students — I started out noting some changes since I was last on campus. But there is one constant – As a member of this community, none of us are sheltered from criminality. We need only walk a block away to experience, in stark terms, the despair and hopelessness of crime, and its root causes, right here in this neighborhood. The answer is not to run away from it, but to use your resources, education, and experiences to increase your civic engagement and help reach truly lasting solutions to these social ills.

To our corporate citizens – the message is the same. You see, our job is not just to prosecute crime, but to deter and prevent criminal conduct. Through our enforcement efforts and our policies, we are committed to incentivizing companies to detect and prevent crime in their own operations, and to come forward and cooperate with us when they identify criminal wrongdoing.

We need corporations to be our allies in the fight against crime.

And we believe that our revised policies will, at the end of the day, further our ability to bring individual wrongdoers — the corporate executives, employees, and agents who engage in misconduct — to justice.

Your resources — particularly your investment in your compliance function — can help increase your corporate civic engagement and lead to lasting solutions to corporate criminality.

Trans Atlantic Collaboration in Crypto Raid

AN OPERATION LED by French and US authorities, strongly supported by Europol, targeted the crypto exchange platform Bitzlato. The globally operating Hong Kong-registered c aryptocurrency exchange is suspected of facilitating the laundering of large amounts of criminal proceeds and converting them into Rubles.Law enforcement authorities took down the digital infrastructure of the service, based in France, and interrogated leading members of the platform's management. The operation also involved law enforcement and judicial authorities from Belgium, Cyprus, Portugal, Spain and the Netherlands.The **Justice Department** announced it arrested Anatoly Legkodymov, 40, a Russian national based in Shenzhen in Miami. He is the founder of Bitzlato, a cryptocurrency exchange that USauthorities described as a "crucial financial resource" to the dark net. Europol reports that about 46 % of the assets exchanged through Bitzlato, worth roughly EUR 1 billion, had links to criminal activities.

In a parallel action, **Treasury's Financial Crimes Enforcement Network (FinCEN)** issued an order that identifies Bitzlato as a "primary money laundering concern" in connection with Russian illicit finance. This is the first order issued pursuant to section 9714(a) of the Combating Russian Money Laundering Act, as amended.

An operation led by French and US authorities, strongly supported by Europol, targeted the crypto exchange platform Bitzlato

EUROPOL.EUROPA.EU

Deputy Treasury Secretary Wally Adeyemo said at a press conference. "Bitzlato has repeatedly facilitated transactions for Russian-affiliated ransomware groups, including Conti, a Ransomware-as-a-Service group that has links to the Russian government and to Russianconnected darknet markets."

Bitzlato received virtual currency worth almost half a billion dollars from illicit activity between 2019 and 2021. Nearly 50 percent of all known Bitzlato transactions during that time involved Russian illicit finance or otherwise risky sources.

As described in the order, Bitzlato is a virtual currency exchange offering exchange and Peer-toPeer (P2P) services. Bitzlato maintains significant operations in and connected to Russia and to Russian illicit finance through its facilitation of deposits and funds transfers by Russia-affiliated ransomware groups or affiliates, and transactions with Russia-connected darknet markets.

FinCEN found that Bitzlato has taken few meaningful steps to identify and disrupt illicit use and abuse of its services. Bitzlato does not effectively implement policies and procedures designed to combat money laundering and illicit finance, and has advertised a lack of such policies, procedures, or internal controls. An internal spreadsheet saved in Bitzlato's shared management folder encapsulated the company's view of itself: "Positives: No KYC. ... Negatives: Dirty money. ..."

Legkodymov is charged with conducting an unlicensed money transmitting business. If convicted, he faces a maximum penalty of five years in prison. The firm's CEO, Financial Director and Marketing director have been arrested by Spanish authorities.

Concurrent with the arrests, French authorities, working with Europol and partners in Spain, Portugal, and Cyprus, dismantled Bitzlato's digital infrastructure, seized Bitzlato's cryptocurrency, and took other enforcement actions.

NASA

University Export Ruse

THE MID-LEVEL PROGRAM administrator responsible for a scheme to export flight control modeling software to a Chinese government entity pleaded guilty Jan 17th. The apparent motive was greed, facilitated by lax accounting and compliance controls.

Between August 2016 and September 2020, Jonathan Yet Wing Soong, 35, was employed as by Universities Space Research Association (USRA), a nonprofit research corporation which leads the NASA Academic Mission Services (NAMS) contract at NASA's Ames Research Center in Mountain View, CA. USRA is contracted by the NASA to, among other things, distribute domestically and internationally sensitive aeronautics-related software developed through the Army's Software Transfer Agreement (STA) program.

As USRA's STA program administrator, Soong was responsible for overseeing certain software license sales, conducting export compliance screening of customers, generating software licenses, and, on occasion, physically exporting software. As part of his duties, Soong was responsible for vetting customers to ensure they did not appear on certain restrictive lists— including the Department of Commerce's Entity List and other U.S. government lists—that placed limitations on the transfer of products to identified entities.

In pleading guilty, **Soong admitted that he willingly exported and facilitated the sale and transfer of restricted software to Beihang University knowing that the university was on the Department of Commerce's Entity List.** Beihang University of Aeronautics and Astronautics BUAA was added to BIS' Entity List in May 2001 due to the University's involvement in People's Republic of China military rocket systems and unmanned air vehicle systems. In 2015 Teledyne LeCroy, a New York Test Equipment manufacturer agreed to settle charges of exporting oscilloscopes to the same entity.

At issue in the case is a software package referred to as CIFER, a tool that allows a user to develop a dynamic model of an aircraft, based on collective flight test data using system identification techniques. According to government filings, the package could be used to analyze and design aircraft control systems.

According to his plea agreement, Soong was aware in April of 2017 that the CIFER software was subject to Export Administration Regulations and that Beihang University was on the Entity List thus making it necessary to obtain a license prior to exporting the CIFER software to the university. Soong acknowledged that he nonetheless arranged to sell and transfer the CIFER software package to the entity without obtaining a license.

Soong acknowledged he used an intermediary to complete the export of the program to avoid detection that the real purchaser was on the Entity List. In May 2017, a representative of the university communicated with Soong and expressed an interest in exploring an arrangement in which rather than use Beihang University as the purchaser of the CIFER software, the purchase would be made in the name of a third-party small company.

For the next several months, Soong communicated with the representative and then, in late 2017, Soong communicated with a representative from Beijing Rainbow Technical Development Ltd. (Beijing Rainbow), identified as being the third-party intermediary for the sale of the CIFER software to Beihang University. Soong ultimately exported directly to Beihang University. In July 2018, Soong also arranged to have the passcodes for the CIFER software package forwarded to Beihang University with

Continues on next page

Continued from previous page

payment coming from Beijing Rainbow.

On September 26, 2022, Soong was charged by information with one count of violating the International Emergency Economic Powers Act (IEEPA), in violation of 50 U.S.C. §§ 1702 and 1705. Pursuant to today's agreement, Soong pleaded guilty to the count. The IEEPA violation carries a statutory maximum penalty of 20 years in prison and a $1,000,000 fine. Sentencing is scheduled for April 28, 2023.

According to reporting at the time of his initial indictment in May 2022, Soong also admitted USRA had not received all the credit card payments made for the software he had exported over the years, and he admitted some of the payments had gone to his personal account.

"He claimed that when customers wanted to pay by credit card, USRA did not have a method set up to accept credit card payments," the complaint states. "He claimed he justified the payments as giving himself a 'bonus,' and estimated he stole 'tens of thousands' over the years."

Danish Freezer Maker Iced

➤ OFAC announced a settlement with Danfoss A/S. a Danish refrigeration manufacturer, with the firm agreeing to pay $4.4 million to settle its potential civil liability for 225 apparent violations of the Iranian Transactions and Sanctions Regulations, the Syrian Sanctions Regulations, and the Sudanese Sanctions Regulations.

The apparent violations occurred when Danfoss FZCO, Danfoss's wholly owned United Arab Emirates (UAE)-based subsidiary, directed customers in Iran, Syria, and Sudan to make payments to its bank account at the UAE branch of a U.S. financial institution. The settlement amount reflects OFAC's determination that Danfoss's apparent violations were non-egregious and not voluntarily self-disclosed. The statutory civil monetary penalty applicable ranged from a base of $21,899,000 to a maximum of $71,383,826.

Aggravating factors included failure to exercise a due degree of caution or care in complying with U.S. sanctions requirements when it used its U.S. Branch Account to receive payments from, and make payments to, customers in sanctioned jurisdictions. Although Danfoss FZCO did not recognize warning signs that such transactions were prohibited, OFAC found no evidence that Danfoss willfully disregarded the relevant prohibitions. By accepting multiple payments from third parties in nonsanctioned jurisdictions, Danfoss FZCO prevented the foreign branch of a U.S. financial institution from appropriately screening and rejecting these transactions; it also enabled businesses in Iran, Syria, and Sudan to engage in international commerce through the U.S. financial system.

Mitigating factors included Danfoss's quick action to ascertain the root causes of the conduct at issue. It also adopted new and more effective internal controls and procedures to prevent a recurrence of the apparent violations, including ceasing doing business entirely in Iran, Syria, and Sudan; new procedures for monitoring and documenting payments to its U.S. bank accounts to identify true originators and reject any payments that originate from a sanctioned jurisdiction; and updating its Export Control Standards and its Export Control Manual to reinforce its employees' understanding of U.S. export controls and sanctions and to help employeesidentify sanctions compliance red flags.

Chipmaking Chemical Broker Convicted

➤ Four and a half years after Customs flagged an attempt to export semiconductor lithography supplies to a barred Chinese Entity, Tao Jiang, 53, of Riverside, CA, and Broad Tech Systems, Inc., pleaded guilty as charged by way of indictment to conspiracy, violation of the Export Control Act, and money laundering conspiracy.

Jiang and Broad Tech System admitted that they conspired together and with Bohr Winn-Shih, an engineer employed at Broad Tech System, to order chemicals from Rhode Island-based FUJIFILM Electronic Materials USA, then knowingly submitted false and misleading documentation to the U.S. Government and to shipping companies in an effort to have those products illegally shipped to a China

Continues on next page

Continued from previous page

Electronics Technology Group Corporation 55th Research Institute, a/k/a Nanjing Electronic Devices Institute (CETC/NEDI) , in violation of the Export Control Reform Act.

CETC/NEDI in Nanjing, China, mainly engages in the manufacturing of electronic components and the research, development and production of core chips and key components in China's military strategic early warning systems, air defense systems, airborne fire control systems, manned space systems, and other national large-scale projects. The Chinese company is on a U.S. government list of businesses that are not permitted to receive products manufactured in the United States.

On October 25, 2018, The Customs and Border Protection National Targeting Center alerted an agent from the Department of Commerce (DOC) of an intended export of 58 gallons of Photoresist to NEDI. The shipment was halted and agents from DOC communicated with FUJIFILM to inform them that NEDI was included on a U.S government list of Chinese companies that U.S companies are prohibited from exporting commodities to. The product was returned to the FUJIFILM.

It is alleged that several days after the shipment to NEDI was halted, the FUJIFILM received a call from Jason Jiang, acting on behalf of Broad Tech System, requesting to purchase 94 gallons of Photoresist. During continuing communications, Jiang and Bohr Winn-Shih represented to the manufacturer that the intended recipient of order, was a company called NTESY, located in Nanjing, China. **The manufacturer communicated to DOC agents that they found this to be suspicious because they had never done business with Broad Tech; ninety-four gallons was a significant quantity of Photoresist; and that the request came just several days after the shipment to NEDI had been recalled.**

Jiang and Broad Tech System are scheduled to be sentenced on April 11, 2023. Jiang's associate, Bohr Winn-Shih, 65, of Ontario, CA, pleaded guilty in May 2021 and was sentenced to one year of probation.

"Talented" GE Engineer Sentenced

➤ A ten-year veteran engineer with General Electric was sentenced to 24 months in prison for conspiring to steal trade secrets, knowing or intending to benefit the People's Republic of China (PRC). Xiaoqing Zheng, 59 of New York, was convicted of conspiracy to commit economic espionage, following a four-week jury trial that ended in March, 2022.

According to court documents, Zheng was employed at GE Power in Schenectady, New York, as an engineer specializing in turbine sealing technology. He worked at GE from 2008 until the summer of 2018. **The trial evidence demonstrated that Zheng and others in China conspired to steal GE's trade secrets surrounding GE's ground-based and aviation-based turbine technologies**, knowing, or intending to benefit the PRC and one or more foreign instrumentalities, including China-based companies and universities that research, develop, and manufacture parts for turbines.

"This is a case of textbook economic espionage. Zheng exploited his position of trust, betrayed his employer and conspired with the government of China to steal innovative American technology," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division.

Assistant Director Alan E. Kohler Jr. of the FBI Counterintelligence Division added "Xiaoqing Zheng was a Thousand Talents Program member and willingly stole proprietary technology and sent it back to the PRC." China introduced the Thousand Talents Plan in 2008 in a bid to lure back ex-patriate scientists and recruit highly-skilled foreign researchers with signing bonuses and prestigious academic appointments.

Former Bolivian Minister of Government gets 70 months

➤ Arturo Carlos Murillo Prijic, 58, was sentenced to 70 months in prison for conspiracy to launder bribes he received in exchange for corruptly helping a U.S. company win a lucrative contract from the Bolivian government. According to court documents, Murillo received at least $532,000 in bribe payments from a Florida-based company in exchange for helping that company secure an approximately $5.6 million contract in 2019 to provide tear gas and other non-lethal equipment to the Bolivian Ministry of Defense.

POLICY BRIEFS

XINJIANG

Wyden Grills Automakers

SENATE FINANCE COMMITTEE Chairman Ron Wyden (D-Ore) is questioning eight major automakers over reports that their supply chains may include materials sourced from the Xinjiang region of China, where forced labor is rampant.

The senator sent letters last week to Ford, General Motors, Honda, Mercedes- Benz, Stellantis, Tesla, Toyota and Volkswagen. His request comes in response to a report by researchers at the Helena Kennedy Centre for International Justice at Sheffield Hallam University that found links between Chinese companies operating in Xinjiang and automakers that import parts from them, including batteries, wiring and wheels.

US law prohibits the importation of goods made with forced labor. "Unless due diligence confirms that components are not linked to forced labor, automakers cannot and should not sell cars in the United States that include components mined or produced in Xinjiang," Sen.

Wyden wrote. "The United States considers the Chinese government's brutal oppression of Uyghurs in Xinjiang an 'ongoing genocide and crimes against humanity.'" Automobiles contains numerous parts sourced from around the world, but "this recognition cannot cause the United States to compromise its fundamental commitment to upholding human rights and US law," he told the automakers.

"The time is now for the auto industry to establish high-road supply chain models outside the Uyghur Region that protect labor and human rights and the environment," said

UAW President Ray Curry. The main lobbying groups for the auto industry had no comment, although MEMA, the Motor & Equipment Manufacturers Association submitted detailed comments to DHS last spring outlining industry's preferred approach to compliance, involving multilateral agreements, the creation of an "approved supplier" and "prohibited/suspected entity/product" lists, and government funding for supply chain tracing technologies.

GERMANY

Supply Chain Law Takes Effect

➤ Called the *Lieferkettengest*, the German Supply Chain Due Diligence Act (GSCA) requires companies to assess human rights and environmental risks across their entire supply chain. It combines various German laws with the intent to eliminate child labor, ameliorate poor labor working conditions, and provide certain environmental protections within global supply chain activities.

The GSCA mandates organizations to generate annual reports on due diligence activities, risk analysis, and risk management actions. These reports must be in German and provide a full audit trail detailing the compliance program's effectiveness, as the organization is expected to show the progress they have made during the year.

Deutsche Welle reports the **EU Draft Directive on Corporate Due Diligence** appears to be even tougher than the German supply chain act. While the German law, for example, doesn't talk of **civil liability in case of violations**, the EU draft includes the possibility for individuals to go to the courts. In addition, corporations from outside the EU, garnering a yet unspecified amount of their revenue in the bloc, will also have to abide by the rules.

EU

Dual Use Consultation

➤ The Commission is collecting and will publish stakeholders' contributions on EU Survey and make them available to the experts of the Member States in the DUCG. The Commission will also publish a summary of the consultation. EU annual export control reports have been prepared since 2013 and include licensing data collected through a dedicated mechanism developed with Member States on a voluntary basis. The EU Dual Use Regulation (EU) 2021/821 (the Regulation) mandates the collection of certain licensing information relevant to the implementation and enforcement of export controls, for reasons of effectiveness, consistency and transparency of export controls inside the EU.

All stakeholders with an interest in export of dual-use items and technologies (e.g. exporters, industry associations, government authorities, academia, research institutions and non-governmental organisations) are invited to provide feedback by submitting comments.

JAPAN

Task Force on Rights and Labor in Supply Chains

➤ United States Trade Representative Katherine Tai and Japan's Minister for Economy, Trade, and Industry Nishimura Yasutoshi signed a Memorandum of Cooperation (MOC) to launch a Task Force on the Promotion of Human Rights and International Labor Standards in Supply Chains.

The Task Force was established under the U.S.-Japan Partnership on Trade. Through the Task Force, the United States and Japan will exchange information on relevant laws, policies, and guidance; facilitate stakeholder dialogues with businesses and worker organizations; and promote best practices for human rights and internally recognized labor rights due diligence.

Continues on next page

Continued from previous page

"The launch of this Task Force is another example of how trade can be a force for good throughout the world. Developing new tools that bring together the combined expertise of agencies across the Governments of the United States and Japan will help contribute to tackling worker exploitation in global supply chains," said **Ambassador Tai**.

On the United States' side, the Task Force is comprised of the Office of the United States Trade Representative, Department of State, Department of Commerce, Department of Health and Human Services, Department of Labor, Department of Homeland Security, U.S. Customs and Border Protection and Immigration and Customs Enforcement, the U.S. Agency for International Development, and other government agencies, as appropriate.

CAATSA

Action on North Korean Labor

➤ U.S. Customs and Border Protection (CBP) began detaining merchandise produced or manufactured by three importers at all U.S. ports of entry on Dec. 5, 2022. This enforcement action is the result of a CBP investigation indicating that these Countering America's Adversaries Through Sanctions Act (CAATSA).

U.S. Customs and Border Protection began detaining merchandise at all U.S. ports of entry from three companies using North Korean labor in their supply chains.
CBP.GOV

Two of the companies, Jingde Trading Ltd. and Zhejiang Sunrise Garment Group Co. Ltd are involved in Auto Parts and T-Shirts, respectively. Specific products of the third firm, Rixin Foods. Ltd could not be identified.

CAATSA prohibits the entry of goods, wares, and articles mined, produced, or manufactured wholly or in party by North Korean nationals or North Korean citizens anywhere in the world, unless clear and convincing evidence is provided that such goods were not made with convict labor, forced labor, or indentured labor under penal sanctions.

CBP will detain merchandise from these entities at all U.S. ports of entry unless there is clear and convincing evidence that forced labor was not present at any stage of the production process. Evidence must be provided within 30 days of notice of detention. If the importer fails to provide clear and convincing evidence within this timeframe, the merchandise may be subject to seizure and forfeiture.

"CBP is committed to keeping America's supply chains free of goods produced with forced labor and to eliminating this horrific practice," said CBP Office of Trade Executive Assistant Commissioner AnnMarie R. Highsmith. "North Korea's forced labor system operates both domestically and internationally and supports the North Korean Government's weapons of mass destruction and ballistic missile programs, and it is also a major human rights violation. Legally and morally, we cannot allow these goods into our commerce."

COMMERCE

Trade Boosted $105 Million to $814 Million

➤ The omnibus spending bill signed by President Biden allocates the Commerce Department $11.2 billion in net discretionary funding, an increase of $1.3 billion above the previous fiscal year, and an additional $1.9 billion in emergency relief funding to respond

Continues on next page

Continued from previous page

to recent natural disasters, and fund scientific and environmental research and other nondefense related programs. BIS funding increased by one-third.

$625 million, $55 million above fiscal year 2022, goes to the International Trade Administration, to help create jobs here at home by increasing U.S. exports, and continued funding for International Trade Administration enforcement and compliance to protect U.S. industries against unfair foreign trade practices.

$191 million, an increase of $50 million above fiscal year 2022, is earmarked for the Bureau of Industry and Security to advance U.S. national security through effective export controls.

DDTC

Updated USPAB Guidance Posted

➤ The Directorate of Defense Trade Controls (DDTC) has updated the guidance for U.S. persons abroad (USPAB) applications.

A U.S. Person Abroad is an individual U.S. person (as defined in ITAR § 120.62) who resides overseas, works for a foreign employer, and provides defense services as defined in ITAR § 120.32(a)(1) and/or (3) to their employer or other foreign parties.

All USPABs require DDTC authorization prior to furnishing defense services to any foreign person. A USPAB authorization does NOT allow for the export of defense articles or the transfer of ITAR-controlled technical data. Such transfers require a separate DDTC authorization.

A new guidance document, as well as a submission letter template and sample §126.13 certification letter for USPAB authorization requests, are located on the DDTC website. Additionally, the USPAB FAQs have been revised and updated.

EXIM

Borneo Refinery Ask Doubled

➤ The Export-Import Bank of the US announced that September's ask for $49 million long-term loan guarantee to support the export of approximately $36 million worth of U.S. engineering services and refining equipment has been doubled. The application is now for a $99.7 million direct loan to support the export of approximately $64 million in U.S. equipment and services. There has been no change in the expected output of the facility.

The Balikpapan Refinery Expansion is being carried out by the refinery's owner, Indonesian state-owned oil and natural gas producer PT Pertamina (Persero). The project is part of the Indonesian government's Refinery Development Master Plan program to revamp and upgrade five refineries in the country.

Pertamina signed a $1.5bn loan agreement with the South Korean Eximbank to finance the Balikpapan refinery expansion in July 2019.

Nikkei Asia reports Pertamina has been struggling to find international partners to jointly invest in projects aimed at upgrading Indonesia's aging refineries. Saudi Aramco pulled out of an upgrade in 2020 at a refinery in Central Java province, after signing a joint venture agreement with Pertamina in 2016. In October 2022 Pertamina announced plans to invest up to $50 billion to build and expand refineries this year, with nearly half ($24 Billion) going to a greenfield project in East Java with Russian state energy company Rosneft.

American engineering consultant Bechtel International carried out the front-end engineering design studies for the Balikpapan project, while Korea's Hyundai Engineering and Australian engineering consultant WorleyParsons are providing engineering, procurement, and construction (EPC) services for the expansion. Suppliers include France's Axens Technologies and Air Liquide for process technologies, UK-based calibration instrument supplier WIKA for site development and construction, and Spain-based oil and gas company Novargi to deliver the waste heat recovery. In 2020 Siemens was awarded the contract to supply compression and power generation equipment.

EXPORT CONTROLS

STATE/DDTC

Seeks Comments on Open GL Recordkeeping

➤ DDTC has launched a pilot program pursuant to its authorities in ITAR § 120.22(b) in order to assess the concept of an Open General License (OGL) mechanism by which it may authorize certain transfers of defense articles to predetermined parties.

DDTC seeks to ensure that persons who rely on any current or future OGLs to conduct reexports and retransfers abroad retain the same records as would be required if their transactions were authorized by either a specific license or an exemption. Accordingly, DDTC has restated the record-keeping requirements articulated in ITAR § 120.15(e) in the OGLs themselves.

BIS

Section 1758 Bio & Toxins Rule Set

➤ The Bureau of Industry and Security (BIS) published the final rule to amend the Export Administration Regulations (EAR) to reflect decisions made at Australia Group (AG) Virtual Implementation Meetings and the AG Plenary Meeting held in July 2022.
The amendments published January 17 include revisions to certain Export Control Classification Numbers to clarify the controls on genetic elements and genetically modified organisms and the scope of the exclusion that applies to medical isolators "specially designed" for barrier nursing or transportation of infected patients; and makes clarifications by adding four naturally occurring, dual-use marine toxins (specifically, brevetoxins, gonyautoxins, nodularins and palytoxin) and removing cholera toxin. The addition of these four toxins is consistent with Section 1758 of the Export Control Reform Act of 2018 (ECRA) regarding emerging and foundational technologies.

Finally, this rule also includes amendments to reflect the AG Plenary updates to the nomenclature of certain bacteria and fungi, and the clarification of the definition of "disinfected" as it applies to certain biological equipment. [88 FR 2507]

DDTC

Voluntary Disclosure – Violations of the Arms Export Control Act

➤ ITAR §127.12 describes the information which should accompany a voluntary disclosure. Historically, respondents to this information collection submitted their disclosures to DDTC in writing via hard copy documentation. However, as part of an IT modernization project designed to streamline the collection and use of information by DDTC, a discrete form has been developed for the submission of voluntary disclosures. [88 FR 2382]

BIS

Chips Rules Add Macau

➤ This rule adds the destination of Macau to the scope of the Regional Stability (RS) controls that were implemented specific to China in the October 7 advanced computing and semiconductor manufacturing equipment rule. For purposes of the EAR, this rule does not change the status of Macau; it will continue to be treated as a separate destination from China. [88 FR 2821]

Wagner Group Sanctioned Further

➤ The Treasury Department's Office of Foreign Assets Control said yesterday it is taking additional actions to degrade Russia's capacity to wage war against Ukraine by expanding sanctions on the para-military Wagner Group. The sanctions target Wagner's key infrastructure and associated front companies, its battlefield operations in Ukraine, producers of Russia's weapons and those administering Russia-occupied areas of Ukraine.

"As sanctions and export controls on Russia from our international coalition continue to bite, the Kremlin is desperately searching for arms and support – including through the brutal Wagner Group – to continue its unjust war against Ukraine," **Treasury Secretary Janet Yellen** said in a statement. "Today's expanded sanctions on Wagner, as well as new sanctions on their associates and other companies enabling the Russian military complex, will further impede Putin's ability to arm and equip his war machine," she continued.

PMC Wagner (Wagner Group) is a Russian private military company led by Yevgeniy Prigozhin, a Putin crony and the target of multiple US sanctions, according to Treasury. Wagner Group has been involved in Kremlin-backed combat operations around the world in support of Putin's war on Ukraine. Treasury stated that as Russia's military has struggled on the battlefield, Putin has resorted to relying on the Wagner Group. The Wagner Group has also meddled and destabilized countries in Africa, committing widespread human rights abuses and extorting natural resources from their people.

Treasury announced that the Wagner Group is being redesignated for being a foreign person that constitutes a significant transnational criminal organization. Wagner personnel have engaged in an ongoing pattern of serious criminal activity, including mass executions, rape, child abductions, and physical abuse in the Central African Republic and Mali. Treasury also is designating numerous entities and individuals on multiple continents that support the Wagner Group's military operations.

'... the Kremlin is desperately searching for arms and support – including through the brutal Wagner Group – to continue its unjust war against Ukraine.'

TREASURY SECRETARY JANET YELLEN

OFAC BRIEFS

Paraguay Politicos

➤ Sanctioned Horacio Manuel Cartes Jara (Cartes), the former Presi-dent of Paraguay, and Hugo Adalberto Velazquez Moreno (Velazquez), the current Vice Presi-dent, for their involvement in the rampant corruption that undermines democratic institutions in Paraguay. OFAC is also designating Tabacos USA Inc., Bebidas USA Inc., Dominicana Acquisi-tion S.A., and Frigorifico Chajha S.A.E., for being owned or controlled by Cartes. These individu-als and entities are being designated pursuant to Executive Order (E.O.) 13818, which builds upon and implements the Global Magnitsky Human Rights Accountability Act and targets per-petrators of serious human rights abuse and corruption around the world.

Marine Safety GL

➤ Authorized through 12:01 a.m. eastern daylight time, April 13, 2023, provided that any payment to a blocked person must be made into a blocked account in accordance with the Global Terrorism Sanctions Regulations: docking, anchoring, crew health and safety, and emergency repairs to eleven vessels owned or controlled by blocked persons. GL 21B does not authorize the offloading of any cargo onboard any of the blocked vessels. [OFAC GL 21B]

Continues on next page

OFAC BRIEFS

Russian Oil Guidance

➤ OFAC issued Preliminary Guidance on Implementation of the Price Cap Policy for Petroleum Products of Russian Federation Origin, giving shippers a window to ship be-fore complying. Russian petroleum products loaded onto a vessel prior to February 5, 2023, and unloaded at the port of destination prior to April 1, 2023, will not be subject to the petroleum products determination.

Oil tanker in the port of Murmansk, Russia
CREATIVE COMMONS, FILE: PETER PROKOSCH

During the specified period U.S. service providers can continue to provide covered services with respect to Russian petroleum products purchased at any price. Once Russian petroleum products or Russian oil are substantially transformed (e.g., subjected to any of the refining processes listed) in a jurisdiction other than the Russian Federation, they are no longer considered to be of Russian Federation origin, and thus the price cap no longer applies. OFAC does not consider blending operations, to be substantial transformation. U.S. persons may reasonably rely upon a certificate of origin but should exercise caution if they have reason to believe such certificate has been falsified or is otherwise erroneous.

Iran Aerospace Executive Sanctions

➤ OFAC) is designating six executives and board members of U.S. designated Qods Aviation Industries (QAI), a key Iranian defense manufacturer responsible for the design and production of unmanned aerial vehicles (UAVs). OFAC is also updating QAI's entry on the Specially Designated Nationals and Blocked Persons List (SDN List) to include its new alias, Light Airplanes Design and Manufacturing Industries. Finally, OFAC is designating the director of Iran's Aerospace Industries Organization (AIO), the key organization responsible for overseeing Iran's ballistic missile programs.

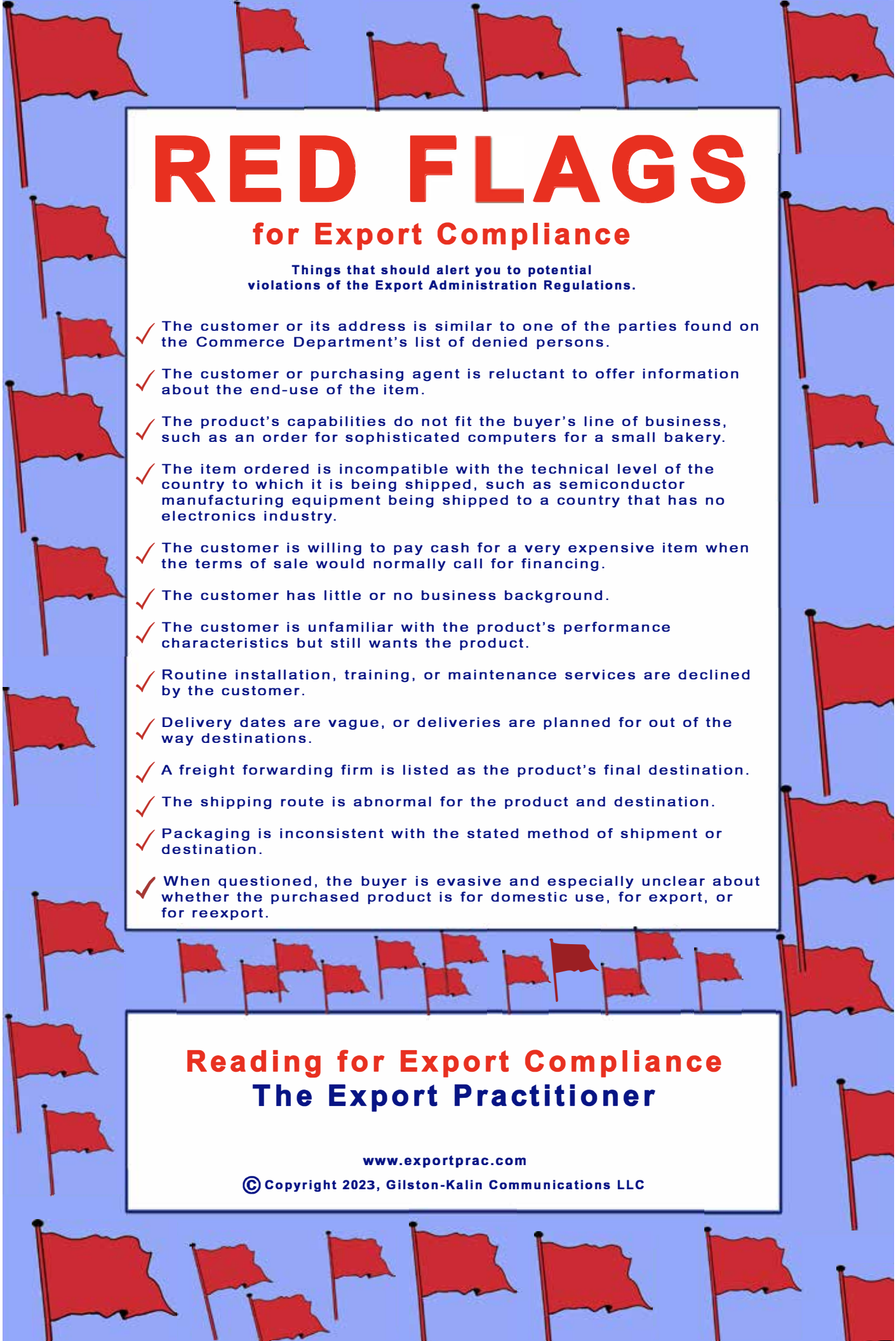
Venezuela GL Updates

➤ Treasury's Office of Foreign Assets Control (OFAC) is publishing two general licenses (GLs) issued pursuant to the Venezuela Sanctions Regulations, each of which was previously made available on OFAC's website. GLs 8K and 41 were issued on November 26, 2022. [88 FR 2237]. GLs 12 and 13 were issued on January 28, 2019. See SUPPLEMENTARY INFORMATION for additional relevant dates. [88 FR 2234] On January 09, 2023, OFAC issued Venezuela-related General License 31B authorizing all transactions involving the IV National Assembly, its Delegated Commission, and others. The IV National Assembly is the opposition body, recognized by the US Government, not the Venezuelan National Constituent Assembly convened by Nicolas Maduro or the National Assembly. [OFAC GL 31B]

Iran FAQ Update

➤ OFAC published one new Iran-related Frequently Asked Question (FAQ 1110) and amending several Iran-related Frequently Asked Questions (FAQs 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 348, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, and 853).

FAQ 1110 addressed technological developments in communication-related soft-ware and services since the issuance of GL D-1 (including in cloud-based services). On September 23, 2022, OFAC issued Iran General License (GL) D-2 to further sup-port the provision of communication tools to ordinary Iranians and assist in their efforts to resist repressive internet censorship and surveillance tools deployed by the Iranian government. OFAC issued GL D-2 to expand and clarify the range of U.S. software and services available to Iranians under OFAC's sanctions program.



RED FLAGS

for Export Compliance

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

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

Reading for Export Compliance

The Export Practitioner

www.exportprac.com