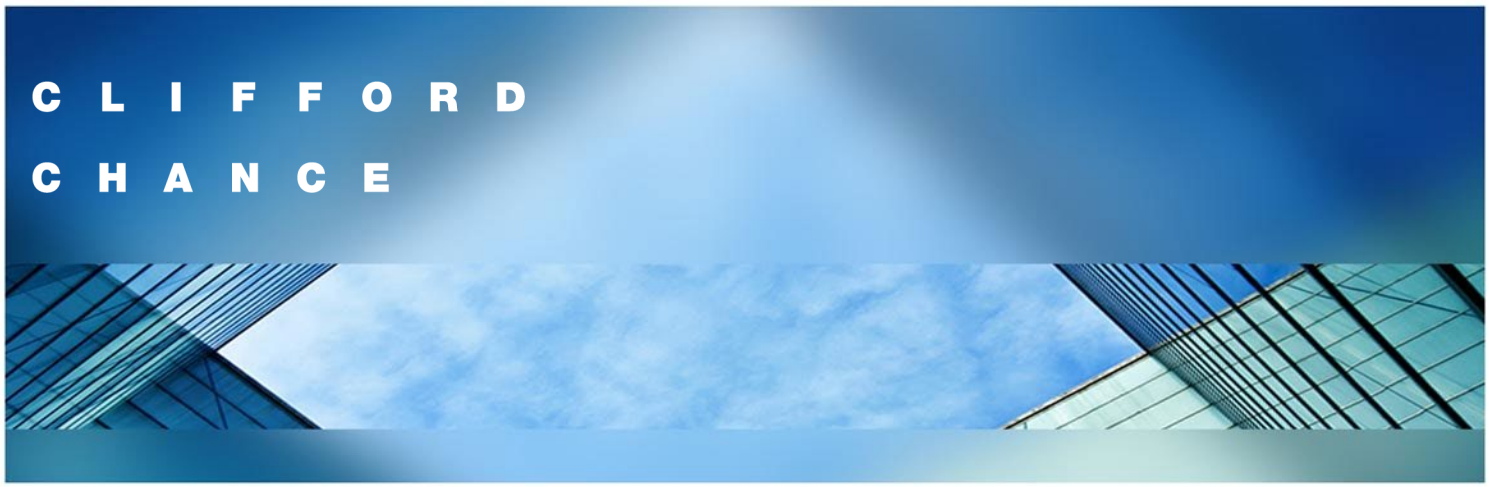

US COMMERCE DEPARTMENT ANNOUNCES LONG ANTICIPATED EXPORT CONTROL ENFORCEMENT WARNING TO FINANCIAL INSTITUTIONS GLOBALLY, RECOMMENDING SPECIFIC ACTIONS TO MANAGE ENFORCEMENT RISK

On October 9, 2024, the US Department of Commerce, Bureau of Industry and Security ("**BIS**") issued, "New Guidance to Financial Institutions on Best Practices for Compliance with the Export Administration Regulations" ("**Guidance**") that, for the first time, expresses an intent by BIS to hold domestic US and non-US financial institutions liable for violations of US export control regulations for which they have provided financing or servicing. While acknowledging that generally the burden and risks for export control violations fall on exporters, BIS warns that given ongoing geopolitical issues, in particular involving Russia and China, they expect all financial institutions to be proactive in detecting and preventing export control violations, including detailed risk management recommendations, or face potential enforcement action. The Guidance follows on prior joint BIS/ Financial Crimes Enforcement Network ("**FinCEN**") guidance to financial institutions emphasizing the parallel anti-money laundering risks for financial institutions processing payments related to export control violations. The Guidance doesn't involve any changes in regulation, but rather signals in very clear language that BIS going forward will use existing authority to hold financial institutions accountable.

The Guidance, which does not incorporate any grace period, assumes a level of US export control expertise that generally is not present in US let alone non-US financial institutions' compliance teams, and presents immediate practical challenges. Nonetheless, all financial institutions should, on a risk basis, consider the specific risk management recommendations contained in the Guidance, and reasonably tailor them as appropriate to the institution's risk assessments and compliance programs going forward. We believe that given the continuing

geopolitical tensions and US national security priorities, export control enforcement against financial institutions is not a question of if but of when.

BIS AND THE EXPORT ADMINISTRATION REGULATIONS

The Export Administration Regulations ("**EAR**"), administered by BIS, "regulate the export, reexport and transfer (in-country) of dual-use items (commodities, software, technology) that have both commercial and military applications, as well as certain less sensitive military items." The EAR apply to any person anywhere in the world, regardless of the transaction currency, if items "subject to the EAR" are involved. This jurisdiction essentially follows the items wherever they may go. Items subject to the EAR include very broad categories, including:

> "all items in the United States, including in a U.S. Foreign Trade Zone or moving in-transit through the United States from one foreign country to another (with certain exceptions); U.S.-origin items wherever located; and certain foreign-made items that incorporate more than a *de minimus* amount of U.S.-origin content or that are produced abroad using U.S. software, technology or tools."

The Guidance specifically advises that under BIS' foreign direct product rules, "nearly all foreign-produced microelectronics and integrated circuits, including items bearing the name of a company headquartered in the United States" are subject to the EAR when destined for Russia, Belarus or Iran, or any Russian or Belarussian "Military End User or Procurement entity" located anywhere.

BIS maintains complex lists of items and persons that are subject to export restrictions – some involving specific countries, end use or end user restrictions, with various levels of license requirements.

HOW DO EXPORT CONTROL REGULATIONS APPLY TO FINANCIAL INSTITUTIONS

The Guidance advises that EAR's General Prohibition 10 ("**GP 10**") prohibits "financial institutions and other persons (regardless of location, country in which they are headquartered or registered, or nationality)" from financing or otherwise servicing, "in whole or in part," any item that is subject to the EAR with "***knowledge***" that a violation of the EAR has occurred, is about to occur, or is intended to occur in connection with the item. Knowledge for these purposes includes not only affirmative knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence. The Guidance states "[s]uch awareness may be inferred from evidence of the conscious disregard of facts known to a person or from a person's willful avoidance of facts."

BIS recognizes in the Guidance that "exporters generally have more information" when it comes to export controls restrictions, but that nonetheless, financial institution's "responsibilities under the EAR have increased significantly." The Guidance then provides specific recommendations of risk management steps that financial institutions on a risk basis should consider to identify and manage red flags of a possible export control violation in order to avoid themselves being charged with a violation.

BIS RECOMMENDS EXPORT RISK-RELATED DUE DILIGENCE TO MITIGATE RISKS OF EXPORT CONTROL VIOLATIONS BY FINANCIAL INSTITUTIONS

Customer Screening: BIS recommends that financial institutions incorporate export control-related due diligence both at the customer onboarding step and as part of regular customer risk assessment activities. This includes customer screening against the lists of restricted parties maintained by BIS, including the BIS Unverified List, Entity List, Military End-User List, and Denied Persons List.[1] BIS further recommends that financial institutions conduct risk-based screening of customers against the lists of entities that have shipped Common High Priority List ("**CHPL**") items to Russia since 2023, according to publicly available trade data.[2] While the Guidance recommends "closely" scrutinizing addresses that have been identified as shipping CHPL items to Russia, financial institutions should use a reasonable and practical risk-based approach.

BIS recommends any hits be assessed and considered both in terms of determining customer risk profiles and for any red flags of export control evasion. BIS cautions that screening should be used as a risk-based tool considering a customer's overall export control-risk profile and potentially as a prompt to ask the customer more questions. Where the results of screening suggest risk or red flags, BIS recommends that financial institutions consider obtaining certifications from the customer regarding the customer's export control compliance and controls to provide the financial institution with adequate assurances. As with sanctions lists, the BIS lists are updated frequently, and this screening should be repeated and kept current.

Transaction Monitoring: BIS recognizes that financial institutions "will likely not have sufficient information to individually assess every transaction for potential EAR violations before processing," but does recommend that financial institutions implement "risk-based procedures . . . to detect and investigate red flags post-transaction" in order to identify and address the risk of possible future violations involving the same parties.

The Guidance identifies critical red flags to be considered, supplementing other red flags identified in prior guidance, including as discussed in our previous alerter here. Generally, while no red flag on its own can confirm a violation or necessarily constitute "knowledge" for purposes of GP 10, the Guidance states certain red flags "demonstrate a high probability of evasion. Financial institutions, like exporters, cannot willfully self-blind or ignore such red flags." The Guidance includes the following examples:

- A customer refuses to provide details to banks, shippers, or third parties, including details about end-users, intended end-use(s), or company ownership.
- The name of one of the parties to the transaction is a "match" or similar to one of the parties on a restricted-party list.

1 The Guidance notes that the Commerce Department maintains a Consolidated Screening List (CSL) that is publicly available.
2 The CHPL is a list developed by the EU, Japan, UK, and US, of certain items that are at high risk of diversion to Russia's military-industrial sector, The CHPL is available here.

- Transactions involving companies that are physically co-located with a party on the Entity List or the SDN List or involve an address BIS has identified as an address with high diversion risk.
- Transactions involving a last-minute change in payment routing that was previously scheduled from a country of concern but is now routed through a different country or company.

BIS further provides guidance on how financial institutions can work to resolve red flags, but most may require discussions with customers to confirm details of the exports.

Real-Time Screening: The Guidance recommends that financial institutions conduct real-time screening of names and addresses for cross-border payments and other transactions "likely to be associated with exports from the United States (or re-exports or in-country transfers outside the United States)" against the following lists:

- The BIS Denied Persons List
- Burmese, Cambodian, Cuban, People's Republic of China (PRC), Iranian, North Korean, Russian, Syrian, Venezuelan, or Belarusian Military-intelligence end users identified in the EAR; and
- Certain persons designated on the Entity List, namely:
    - Entities subject to the Entity List Foreign Direct Product (FDP) rule and designated with a footnote 4 in the license requirement column of the Entity List;
    - Entities subject to the Russia/Belarus-Military End User and Procurement FDP rule, and designated with a footnote 3 in the license requirement column of the Entity List; and
    - Other persons included on the Entity List and subject to the license review policies related to certain rocket systems and unmanned aerial vehicles, and chemical and biological weapons end-uses).

BIS recommends that this real-time screening include all parties to a transaction of which the financial institution has actual knowledge in the ordinary course of its business, including the ordering customer and beneficiary customer in an interbank financial message. Significantly, the Guidance states "BIS does not expect financial institutions to request additional names of parties for the sole purpose of conducting this real-time screening, although financial institutions may not willfully self-blind or deliberately avoid becoming aware of facts or circumstances, as doing so may itself demonstrate "knowledge" for purposes of GP 10."

Where a financial institution finds a match in this circumstance, BIS recommends that the financial institution not proceed with the transaction unless and until it can determine that the transaction is in compliance with the EAR. "Failure to do so risks liability for a knowing violation of the EAR under GP 10."

VOLUNTARY DISCLOSURES

Like many US enforcement authorities, BIS encourages financial institutions that have identified a violation to come forward and voluntarily disclose the violation to BIS. Unlike other US enforcement agencies, BIS has stated that it will consider it an aggravating circumstance if a financial institution decides not to voluntarily disclose an identified violation and BIS later learns of it, rendering such disclosures perhaps a little less than voluntary. See our prior alerter on this issue here.

ENFORCEMENT JURISDICTION AND PENALTIES

BIS has extraterritorial jurisdiction, and the EAR applies globally whenever items subject to the EAR are involved (and also to certain US person activity, regardless of the involvement of EAR items). Therefore, as noted above, US and non-US financial institutions may have compliance risk whenever their transactions and related activities implicate the EAR. Violations of the EAR can result in civil fines up to approximately USD 360,000 per violation or twice the value of the transaction, whichever is greater. In addition, criminal penalties (i.e., where persons act with knowledge) can be imposed by the US Department of Justice of up to USD 1 million per violation and/or up to 20 years imprisonment (for individuals). Violations also can result in the denial of export privileges, reputational harm, and business disruptions.

KEY TAKEAWAYS FOR FINANCIAL INSTITUTIONS

While this Guidance has been long foreshadowed, the escalating US national security concerns involving Russia and China have now led to BIS fully deputizing global financial institutions to enforce US export control requirements under penalty of prosecution. Both domestic and non-US financial institutions should carefully assess BIS' express risk management recommendations. They should tailor them to their risk profile and business, while incorporating them as appropriate into their customer and enterprise-wide risk assessments and compliance programs. Failure to take and to documents reasonable steps to do so leaves the financial institution vulnerable to BIS and potentially DOJ enforcement.

CONTACTS

David DiBari
Partner

T +1 202 912 5098
E david.dibari
@cliffordchance.com

Renée Latour
Partner

T +1 202 912 5509
E renee.latour
@cliffordchance.com

Michelle Williams
Partner

T +1 202 912 5011
E michelle.williams
@cliffordchance.com

Holly Bauer
Associate

T +1 202 912 5132
E holly.bauer
@cliffordchance.com

Joshua Berman
Partner

T +1 202 912 5174
E joshua.berman
@cliffordchance.com

George Kleinfeld
Partner

T +1 202 912 5126
E george.kleinfeld
@cliffordchance.com

John-Patrick Powers
Partner

T +1 202 912 5048
E john-patrick.powers
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Jamal El-Hindi
Counsel

T +1 202 912 5167
E jamal.elhindi
@cliffordchance.com

Vasu Muthyala
Partner

T +65 6661 2051
E vasu.muthyala
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 2001 K Street NW, Washington, DC 20006-1001, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Riyadh* • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

*AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.