October 15, 2024

Commerce's BIS Issues Guidance to Financial Institutions on Export Control Compliance

On October 9, 2024, the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") issued guidance to financial institutions on "best practices" for compliance with the Export Administration Regulations ("EAR"), including General Prohibition 10.[1] The Guidance appears to mark the first time that BIS has formally indicated that U.S. and non-U.S. financial institutions could be the subject of enforcement actions by BIS for violating the export control regulations directly.

Overview

In the context of the U.S. government's response to Russia's invasion of Ukraine in 2022, FinCEN and BIS issued joint guidance documents in 2022 and 2023 encouraging U.S. financial institutions for the first time to monitor for potential violations of export controls and to report those violations under their pre-existing obligations under the Bank Secrecy Act and applicable anti-money laundering laws to file Suspicious Activity Reports ("SARs").[2] Many financial institutions responded to this new imperative by making substantial compliance changes, given that financial institutions had traditionally not focused on monitoring for potential export control violations by their customers. Assistant Secretary for Export Enforcement Matthew Axelrod has prioritized engagement with the financial services community, noting, for example, that "when an advanced semiconductor moves from the U.S. to China—there's a financial side of that transaction."[3]

The Guidance ratchets up BIS's focus on financial institutions by formally indicating, apparently for the first time, that BIS may bring enforcement actions against financial institutions for directly violating the export control regulations, and in particular General Prohibition 10 of the EAR ("GP 10"). GP 10 includes a prohibition on "servic[ing]" a transaction "with knowledge" that it has or will violate the EAR.[4] This includes a prohibition on "financ[ing]" such a transaction. As the Guidance notes, "knowledge" can include "an awareness of a high probability of [a circumstance's] existence or future occurrence" that can be "inferred from

---

1 U.S. Dep't of Commerce, *Bureau of Industry and Security Issues New Guidance to Financial Institutions on Best Practices for Compliance with the Export Administration Regulations* (Oct. 9, 2024), available here (the "Guidance"); *see also* Press Release, available here.

2 Paul, Weiss, *FinCEN and BIS Issue Joint Notice Emphasizing That Financial Institutions Should Monitor for Possible Export Control Violations* (Nov. 14, 2023), available here.

3 Compliance Week, *BIS's Axelrod makes plea to financial services: 'We want to work with you'* (June 12, 2024), available here.

4 General Prohibition 10 relates to: "Proceeding with transactions with knowledge that a violation has occurred or is about to occur (Knowledge Violation to Occur)." It states: "You may not sell, transfer, export, reexport, finance, order, buy, remove, conceal, store, use, loan, dispose of, transport, forward, or otherwise service, in whole or in part, any item subject to the EAR and exported, reexported, or transferred (in-country) or to be exported, reexported, or transferred (in-country) with knowledge that a violation of the Export Administration Regulations, the Export Control Reform Act of 2018, or any order, license, license exception, or other authorization issued thereunder has occurred, is about to occur, or is intended to occur in connection with the item. Nor may you rely upon any license or license exception after notice to you of the suspension or revocation of that license or exception. There are no license exceptions to this General Prohibition Ten in part 740 of the EAR." 15 C.F.R. § 736.2.

evidence of the conscious disregard of facts known to a person or from a person's willful avoidance of facts." While GP 10 is longstanding and applies broadly to all types of entities, the traditional understanding as of several years ago was that BIS was not actively seeking to bring enforcement cases against financial institutions under GP 10.

The Guidance makes clear that BIS is now squarely focused on financial institutions' obligations under the EAR itself. In fact, the Guidance states that while export controls compliance "has traditionally been of greatest concern to exporters," financial institutions' "responsibilities under the EAR have increased significantly" in recent years following Russia's 2022 invasion of Ukraine and the increased U.S. restrictions on China.

The Guidance describes best practices in three categories for avoiding violations of GP 10: 1) export-control related customer due diligence; 2) post-hoc review of transactions for red flags of potential export control violations; and 3) real-time screening in limited circumstances. We review each of these in more detail below. We expect that many financial institutions will need to expend substantial effort to fully adopt these best practices.

Importantly, unlike the SAR-filing obligation, GP 10 applies to all entities, including non-U.S. financial institutions, that may finance or otherwise service transactions involving items subject to the EAR (which include most U.S.-manufactured items and certain categories of items manufactured outside the United States). Some of BIS's most significant enforcement resolutions in the past have been with non-U.S. entities.

Customer Due Diligence

BIS recommends that financial institutions incorporate export controls due diligence when "onboarding a new customer and as part of regular risk-based due diligence thereafter."[5]

- *BIS Restricted Party Lists*: BIS suggests that financial institutions conduct customer screening against lists of persons subject to BIS's end-user restrictions, such as the Unverified List, Entity List, Military End-User List, and Denied Persons List.[6] BIS recommends that financial institutions "heavily weigh" a customer's presence on this list in determining the "customer's overall risk profile for potential EAR violations[.]"

- *Trade Data Screening*: BIS recommends screening "customers—and, where appropriate, customers' customers—against lists of entities that have shipped Common High Priority List (CHPL) items to Russia since 2023, according to publicly available trade data" available through sources such as the Trade Integrity Project from the Open-Source Centre. BIS recommends that financial institutions "closely scrutinize entities or addresses identified as shipping CHPL items to Russia to determine whether any circumstances indicating export control evasion ('red flags') are present."

While the presence of an entity on a BIS list or other lists would not prohibit the financial institution from providing services, BIS recommends that, when an entity is on such a list, the financial institutions take further steps to "determine whether the customer is engaged in the export, reexport, or transfer of items subject to the EAR." If so, BIS recommends that financial institutions ask the customer to "certify whether it has sufficient controls in place to comply with the EAR[.]"

[5] BIS notes that this screening should be done not only "at onboarding" but also on an ongoing "regular basis" because the restricted lists are "updated continuously to add and remove parties."

[6] BIS recommends utilizing Commerce's Consolidating Screen List, which also includes persons listed by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), and the Department of State's Directorate of Defense Trade Controls ("DDTC").

Post-Hoc Review of Transactions for Red Flags for Export Control Violations

Apart from performing real-time screening in the limited circumstances described below, BIS notes that financial institutions "will likely not have sufficient information to individually assess every transaction for potential EAR violations before proceeding[.]" Accordingly, "BIS **does not** expect [financial institutions] to review transactions for these red flags in real time."[7]

However, BIS does expect financial institutions to have "risk-based procedures in place to detect and investigate red flags post-transaction and, if necessary, take action to prevent violations of the EAR before proceeding with any transactions involving the same customer or counterparties." These "red flags" have been identified in BIS's prior joint guidance with FinCEN. BIS notes that while "no single financial red flag is necessarily indicative of illicit or suspicious activity" there are certain red flags that, if detected during a post-transaction review, should be "sufficient" for the financial institution to avoid engaging in further transactions with that customer.[8] In these circumstances, BIS recommends that the financial institution "resolve" those red flags before engaging in further transactions with the customer, such as by "obtaining a copy of the export licensed issued by BIS."

Real-Time Screening in Limited Circumstances

BIS emphasizes that, as a general matter, "in recognition of difficulties in implementation, BIS does not expect [financial institutions] to engage in real-time screening of parties to a transaction[.]" However, BIS does "recommend[] real-time screening against the names and addresses" on certain BIS lists, including the BIS Denied Persons List.[9] BIS recommends that this real-time screening "include all parties to a transaction of which [a financial institution] has actual knowledge in the ordinary course of its business, including the ordering customer and beneficiary customer in an interbank financial message."[10] If there is a match, BIS recommends that the financial institution decline to proceed with the transaction until it can determine that it is authorized under the EAR.

Takeaways

In addition to complying with FinCEN and BIS guidance on filing SARs regarding export control evasion, U.S. financial institutions—and now non-U.S financial institutions—should give consideration to measures to avoid direct violations of GP 10. U.S. and non-U.S. financial institutions engaged in international transactions should also consider reviewing which of the "best practices" described by BIS they currently follow, and what steps would be necessary to close any gaps. We expect that many financial institutions would need to take additional measures to fully align with BIS's new guidance. Financial institutions will also experience an additional burden if the banking agencies begin to incorporate this guidance into their examinations.

---

7 Guidance (emphasis added).

8 The Guidance notes that the presence of such a red flag may be "sufficient" for knowledge under GP 10. Those flags are: (i) the "customer refuses to provide details to banks, shippers, or third parties, including details about end-users, intended end-use(s), or company ownership"; (ii) 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"; (iii) "[t]ransactions 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" and (iv) "[t]ransactions 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."

9 The Guidance also suggests including the following in real-time screening: (i) "Burmese, Cambodian, Cuban, People's Republic of China (PRC), Iranian, North Korean, Russian, Syrian, Venezuelan, or Belarusian Military-intelligence end users identified in 15 CFR 744.22(f)(2)" and (ii) "[c]ertain persons designated on the Entity List, namely: [a] Entities subject to the Entity List Foreign Direct Product (FDP) rule, 15 CFR 734.9(e), and designated with a footnote 4 in the license requirement column of the Entity List in supplement no. 4 to part 744 of the EAR; [b] Entities subject to the Russia/Belarus-Military End User and Procurement FDP rule, 15 CFR 734.9(g), and designated with a footnote 3 in the license requirement column of the Entity List in supplement no. 4 to part 744 of the EAR; and [c]Other persons included on the Entity List and subject to the license review policy set forth in 15 CFR 744.2(d) (related to certain nuclear end uses), 15 CFR 744.3(d) (related to certain rocket systems and unmanned aerial vehicles end uses), and 15 CFR 744.4(d) (related [sic] certain chemical and biological weapons end-uses)."

10 BIS notes that it does not expect financial institutions "to request additional names of parties for the sole purpose of conducting this real-time screening" but notes that 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."

In addition, as the Guidance notes, financial institutions should consider whether to file voluntary self-disclosures ("VSDs") if they suspect that they have violated the export control regulations. For example, it would be prudent for a financial institution to consider a VSD when filing a SAR for a suspected or actual export control violation if the financial institution determines it had, or should have had, knowledge of the violation at the time of the transaction. Financial institutions should bear in mind that, unlike OFAC and certain other agencies, BIS will view it as an aggravating factor if a party fails to file a VSD where the potential violation is "significant" in nature.[11]

* * *

[11] Paul, Weiss, *BIS Imposes $300 Million Penalty Against Seagate for Export Control Violations and Makes Controversial Changes to Voluntary Self-Disclosure Program* (May 1, 2023), available here.

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

L. Rush Atkinson
+1-202-223-7473
ratkinson@paulweiss.com

Jessica S. Carey
+1-212-373-3566
jcarey@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Elizabeth Hanft
+1-212-373-3664
ehanft@paulweiss.com

Brad S. Karp
+1-212-373-3316
bkarp@paulweiss.com

Loretta E. Lynch
+1-212-373-3000

Nicole Succar
+1-212-373-3624
nsuccar@paulweiss.com

Samuel Kleiner
+1-212-373-3797
skleiner@paulweiss.com

Nathan Mitchell
+1-202-223-7422
nmitchell@paulweiss.com

Associates Sean S. Malone, Samuel Rebo, and Joshua Thompson contributed to this Client Alert.