Bureau of Industry and Security Issues New Guidance to Financial Institutions on Best Practices for Compliance with the Export Administration Regulations

This notice provides guidance to financial institutions (FIs) on best practices to ensure compliance with the Export Administration Regulations (EAR, 15 CFR Parts 730-774), administered and enforced by the U.S. Department of Commerce, Bureau of Industry and Security (BIS). While EAR compliance has traditionally been of greatest concern to exporters, FIs' responsibilities under the EAR have increased significantly following Russia's further invasion of Ukraine in 2022 and the enhanced national security and foreign policy imperative to restrict China's military modernization efforts and commission of human rights violations. The guidance below highlights best practices that FIs should adopt in order to minimize their risks of violating the EAR, including General Prohibition 10 (GP 10).

After providing background on the EAR, this guidance provides BIS's best practice recommendations – regarding EAR-related due diligence, ongoing reviews of transactions, and real-time screening – that will allow FIs to reduce the risk of an inadvertent violation of the EAR. Consistent with prior joint notices issued by BIS and the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), FinCEN expects FIs to report suspicious activity related to potential EAR violations. FinCEN has further requested that FIs utilize key terms in Suspicious Activity Reports (SARs) related to potential violations of the EAR.[1]

Background on the EAR, General Prohibition 10, and U.S. Persons Controls

The EAR 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. BIS has authority over transactions involving items that are "subject to the EAR," even when no U.S. person or U.S. financial institution is involved in the transaction. Items "subject to the EAR" include 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 minimis* amount of U.S.-origin controlled content or that are produced abroad using controlled U.S. software, technology or tools.

[1] For potential Russian and Belarusian export control evasion attempts, FinCEN requests FIs file SARs using the key term "FIN-2022-RUSSIABIS"in SAR field 2 (Filing Institution Note to FinCEN) and the narrative. For potential export control evasion attempts involving any other part of the world, FinCEN requests FIs file SARs using the key term "FIN-2023-GLOBALEXPORT".

BIS recognizes that exporters generally have more information than FIs about whether an item may be subject to the EAR. That said, FIs should be aware that items shipped from the United States are generally subject to the EAR, with narrow exceptions.[2] In addition, under BIS's foreign direct product rules, nearly all foreign-produced microelectronics and integrated circuits, including items bearing the brand name of a company headquartered in the United States, are subject to the EAR when destined for Russia, Belarus, or Iran, or a Russia/Belarus-Military End User or Procurement entity anywhere in the world, regardless of where such items are manufactured.

Under GP 10, FIs and other persons (regardless of location, country in which they are headquartered or registered, or nationality) may not finance or otherwise service, in whole or in part, any item 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. In addition, U.S. persons, wherever located – including FIs – may not support (*e.g.*, finance or facilitate) certain specified activities that they know involve certain WMD or military-intelligence programs.[3] In both instances, "knowledge" of a circumstance includes not only positive 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. Such 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.

How EAR-Related Due Diligence Best Practices Can Help Avoid Violations of GP 10

To avoid potential violations of GP 10 of the EAR, BIS recommends that FIs incorporate EAR-related due diligence into their risk management and compliance processes, both before onboarding a new customer and as part of regular risk-based due diligence thereafter.

BIS recommends that such EAR-related due diligence include reviewing customers 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. In particular, BIS's restricted-party lists feature their own specific set of license or other EAR requirements for transactions involving listed parties. To assist the public with screening against relevant export-related U.S. government restricted-party lists, the Department of Commerce maintains the Consolidated Screening List (CSL), which includes persons listed by BIS, 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).

While being subject to BIS's end-user restrictions does not by itself prevent a party from receiving services from FIs, BIS nevertheless recommends that FIs heavily weigh a customer's

[2] Items not subject to the EAR include but are not limited to items subject to the jurisdiction of another agency, such as defense articles, commodities related to nuclear reactor vessels, special nuclear materials, as well as certain information and software that are published or arise during fundamental research. *See* 15 CFR 734.3(b).
[3] 15 C.F.R. § 744.6(b).

presence on a BIS restricted-party list when determining the customer's overall risk profile for potential EAR violations—including in connection with the receipt of services.

In addition to screening customers against BIS restricted-party lists, BIS recommends as an EAR-related due diligence best practice that FIs review 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. Such lists can be obtained from commercial service providers or free of charge from the Trade Integrity Project (TIP), an initiative of the U.K.-based Open-Source Centre. Consistent with BIS guidance on the use of such trade data, FIs should 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.

When a customer is on a BIS restricted-party list or a list of entities that have shipped CHPL items to Russia, BIS recommends that FIs determine whether the customer is engaged in the export, reexport, or transfer of items subject to the EAR. If so, BIS recommends that FIs ask that customer to certify whether it has sufficient controls in place to comply with the EAR, including screening transactions against lists of persons subject to BIS's end-user restrictions; exercising heightened due diligence for exports, reexports, or transfers to destinations subject to BIS-administered embargoes or broad trade restrictions, such as Russia; and engaging in enhanced due diligence processes for items included on the Commerce Control List (CCL) (Supplement No. 1 to Part 774 of the EAR), or the CHPL.

EAR-related due diligence, of course, is not a one-and-done process. The restricted-party lists BIS maintains under the EAR and other publicly available red flag lists based on trade data are updated continuously to add and remove parties. BIS recommends that FIs check these lists on a regular basis to ensure they have the most up-to-date information informing the risk profiles of both their customers and their customers' customers.

How Ongoing Reviews of Transactions for Red Flags Can Help Avoid Violations of GP 10

In addition to engaging in EAR-related due diligence when onboarding and retaining customers, BIS recommends that, in order to minimize the potential for violations of GP 10, FIs review transactions on an ongoing basis for red flags. BIS recognizes that FIs will likely not have sufficient information to individually assess every transaction for potential EAR violations before proceeding (subject to the exceptions for real-time screening outlined below); accordingly, BIS does not expect FIs to review transactions for these red flags in real time. Nevertheless, an FI may learn of information that constitutes a red flag after it has processed payment for a transaction, which may give rise to "knowledge" for purposes of GP 10 for future transactions involving the same customer or counterparties. Accordingly, BIS recommends that FIs 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.

BIS and FinCEN have issued previous joint notices identifying red flags to assist FIs in identifying transactions potentially tied to the evasion of U.S. export controls. Consideration of these indicators, as well as those set out in the prior joint FinCEN-BIS alerts pertaining to Russia-related export control evasion, can assist in determining whether an identified activity may be connected to evasion of U.S. export controls. As no single financial red flag is necessarily indicative of illicit or suspicious activity, all of a transaction's surrounding facts and circumstances should be considered when determining whether a specific transaction is suspicious or associated with potential export control evasion.

That said, the presence of certain individual red flags may be sufficient to constitute "knowledge" under the EAR. As noted above, knowledge of a circumstance includes not only positive 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. Certain red flags – including the ones noted below – demonstrate a high probability of evasion. FIs, like exporters, cannot willfully self-blind or ignore such red flags.

If, during a post-transaction review, an FI encounters one of the below red flags and cannot resolve it to its satisfaction, BIS recommends that the FI refrain from future transactions with the relevant transaction parties. Otherwise, the FI risks liability for a violation of the EAR under GP 10:

- 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.
- 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.

FIs can resolve these red flags by, among other things, confirming that the item exported, reexported, or transferred (in country) is not subject to the EAR, outside the scope of the license requirement triggered by a party's inclusion on a restricted-party list, or otherwise authorized by a BIS license exception or license. BIS recognizes that exporters generally have more information than FIs about whether an item may be subject to the EAR and generally rely on their customers' representations regarding compliance with the EAR, unless such reliance would be unreasonable – for example, when the FI has reason to know that such representations may be false.

BIS does not generally authorize transactions that would otherwise be prohibited by GP 10. BIS also does not confirm the existence of a license to third parties. Accordingly, FIs should seek confirmation from their customers regarding BIS-issued licenses, including by obtaining a copy

of the export license issued by BIS. If provided with an Application Control Number (ACN) or Case Number, an FI can track the status of an export license application using the System for Tracking Export License Applications (STELA).

The Bureau of Industry and Security actively encourages the submission of Voluntary Self-Disclosures (VSDs) from parties who suspect they may have violated the EAR. Parties are strongly encouraged to submit VSDs electronically to BIS_VSD_INTAKE@bis.doc.gov.

In certain circumstances, following an FI's filing of a SAR with FinCEN, BIS may provide the FI with additional information that would establish knowledge that a violation of the EAR has occurred, is about to occur, or is intended to occur. In such circumstances, to avoid violating GP 10, BIS expects the FI to take steps necessary to ensure that it does not finance or otherwise service items exported (or reexported or transferred in-country) in violation of the EAR in the future, including, if appropriate, by terminating a customer relationship.

How Real-Time Screening Can Help Avoid Violations of GP 10

Generally, in recognition of difficulties in implementation, BIS does not expect FIs to engage in real-time screening of parties to a transaction to prevent violations of GP 10. Instead, BIS recommends that FIs implement the EAR-related due diligence and ongoing review for red flags described above to avoid financing or servicing a transaction with "knowledge" in violation of GP 10.

BIS does, however, recommend real-time screening against certain BIS-administered restricted-party lists in certain circumstances to avoid potential violations of GP 10.[4] Specifically, for cross-border payments and other transactions that are likely to be associated with exports from the United States (or re-exports or in-country transfers outside the United States), BIS recommends real-time screening against the names and addresses on the following lists:

- The BIS Denied Persons List, *see* 15 CFR Part 764, Supplement No. 1;
- 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
- Certain persons designated on the Entity List, namely:
    - 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;
    - 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

[4] Note that certain of these restricted parties are identified on the CSL – BIS considers transactions involving these restricted parties to be of particularly high risk of involving a GP 10 violation.

- 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 certain chemical and biological weapons end-uses).

BIS recommends that this real-time screening include all parties to a transaction of which an FI has actual knowledge in the ordinary course of its business, including the ordering customer and beneficiary customer in an interbank financial message. BIS does not expect FIs to request additional names of parties for the sole purpose of conducting this real-time screening, although FIs 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 circumstances where there is a match to a party on one of the lists set forth above, BIS recommends that FIs decline to proceed with a transaction until the FI can determine that the underlying export, reexport, or transfer (in-country) is authorized under the EAR (or alternatively not subject to the EAR). Failure to do so risks liability for a knowing violation of the EAR under GP 10. Consistent with the prior joint notices issued by BIS and FinCEN, BIS expects FIs to report all suspicious activity related to EAR violations using the appropriate SAR terms. BIS also actively encourages the submission of Voluntary Self-Disclosures (VSDs) from parties who suspect they may have violated the EAR. FIs can submit VSDs electronically to BIS_VSD_INTAKE@bis.doc.gov.