



Financial Institutions Face Greater Export Controls Compliance Risk Under New BIS Guidance

11 November 2024

Financial institutions face significant new compliance obligations under export control [guidance](#) issued by the Commerce Department's Bureau of Industry and Security (BIS) last month. With a focus on exports to Russia and China, BIS has:

- Prioritized enforcement against financial institutions that provide services if they have reason to know an underlying transaction violates export controls.
- Established that BIS will consider financial institutions to have had reason to know the unlicensed supply of *any* semiconductors to Russia violates export controls.

Given the broad reach of U.S. export controls, both U.S. and non-U.S. financial institutions should evaluate and consider bolstering their transaction screening and other compliance procedures.

A Departure From Traditional Practice

The law has always required financial institutions to comply with applicable U.S. export controls. That includes General Prohibition 10 (GP 10), which prohibits:

- Financing or servicing any item subject to U.S. export controls with knowledge or reason to know a violation of export controls has occurred or will occur.
- Financing or facilitating certain activities with knowledge or reason to know they involve weapons of mass destruction or military-intelligence programs.

A Key Change

BIS expects financial institutions to detect and report potential export control violations. However, it has not traditionally sought to hold financial institutions liable under GP 10.

Past practice: Financial institutions typically have relied on information from exporters to comply with export controls. The rationale was that exporters generally have more information about whether an item is subject to export controls.

- Within the past several years, BIS and the Treasury Department’s Financial Crimes Enforcement Network have issued a series of guidance about “red flags” that may signal export control evasion.
- Such guidance emphasized the importance of detecting and reporting suspicious activity, including through a financial institution’s trade finance activities, as part of an institution’s Bank Secrecy Act (BSA)/anti-money laundering compliance program.

Future focus: BIS is shifting its approach. It now expects financial institutions to perform export-related due diligence, screen against BIS restricted party lists and monitor transactions rather than generally relying on information from an exporter.

Key Components of a Robust Export Compliance Program for Financial Institutions

BIS recommends that financial institutions take steps to identify customers, counterparties and transactions that pose higher risks. It encourages them to focus on the following areas:

1. Due Diligence

BIS urges financial institutions to:

- Screen all known parties to the transaction.
 - BIS urges real-time screening against BIS-administered restricted party lists, such as the Unverified List, Entity List, Military End-User List and Denied Persons List, for cross-border payments and other transactions likely associated with exports from the United States.
 - If a financial institution identifies a match in real-time, it should stop to investigate and proceed only if the export is authorized.
- Review customers and, where appropriate, customers’ customers, against lists of entities that have shipped [Common High Priority List](#) (CHPL) items to Russia since 2023 to detect any export control evasion red flags.

Resolving screening matches and investigating red flags may require financial institutions to train and possibly add employees.

Financial institutions generally may provide services unrelated to export transactions to persons included on BIS restricted party lists. However, BIS recommends that financial institutions:

- Heavily weigh a party’s inclusion on one of such lists in determining a customer’s risk profile.
- Determine whether such customers are engaged in the export, reexport or transfer of items subject to U.S. export controls, and if so, ask them to certify as to sufficient controls in place to ensure export control compliance measures, such as screening against BIS restricted party

lists and conducting heightened due diligence for destinations such as Russia and for CHPL items.

2. Ongoing Transaction Review for Red Flags

With the exception of screening against restricted party lists, BIS generally does not expect financial institutions to review transactions for export controls red flags in real time. However, BIS recommends risk-based procedures to help institutions detect and resolve red flags discovered post-transaction.

BIS expects that financial institutions act to prevent U.S. export control violations before engaging in future transactions involving the same customer or counterparty that was involved in a prior transaction that raised red flags, including, if appropriate, by terminating a customer relationship. If a financial institution engages in transactions with a customer or counterparty that has unresolved red flags, BIS will impute knowledge of a violation to an institution.

The BIS guidance includes red flags that indicate a “high probability” of export control evasion, including:

- A refusal to provide details about end-users, end-use or company ownership.
- A match or close match with a name on a restricted party list.
- An address match with parties on the Entity List or OFAC’s SDN List.
- Last-minute changes in payment routing from a country of concern to a different country or company.

Financial institutions may resolve red flags by confirming a given item is not subject to U.S. export controls or that the transaction is authorized, including by requesting a copy of a license. Financial institutions can rely on a customer’s representation unless they have reason to know it may be false.

Practical Considerations: 9 Things Financial Institutions Should Consider

BIS provides little detail on how institutions should implement the guidance, although it will require significant cost, time and effort for most. U.S. financial institutions should consider the following steps:

1. Assess the institution’s exposure to cross-border payments and trade activity, particularly with respect to Russia and China. Calibrate compliance measures.
 - For example, a retail-focused community bank is much less likely to face exposure to export control risks than a bank with a significant trade finance operation.
 - Given BIS’s focus on Russia and China, risk-based compliance measures should adequately cover those geographies.

2. Identify customers or customer segments active in international exports and trade, particularly those involving Russia and China, as well as customers more likely to deal in items subject to U.S. export controls.
3. Identify whether the institution uses BIS-administered restricted party lists to screen customers and transactions. If not, commence using them as appropriate.
4. Adopt or amend policies and procedures that reflect a commitment to export control compliance. Raise awareness among employees of export control requirements.
5. Assess the expertise of employees to analyze flagged transactions. Supplement as necessary.
6. Consider how red flags mentioned in past regulatory communications may apply. Document conclusions and rationale.
7. Consider using or adjusting algorithms for transaction monitoring tools to monitor for red flags.
8. Verify the effectiveness of internal escalation mechanisms.
9. Identify customers and transactions to screen against the additional lists on a risk basis.

Next Steps

What we know:The guidance notes repeatedly that failing to implement effective compliance controls increases the risk of violating GP 10.

- The guidance follows a recent [BIS final rule](#) that increased penalty caps. The rule also provided BIS more discretion in resolving enforcement matters.
- Taken together, the pronouncements signal an intent to step up enforcement.

What we don't know:It is unclear how assertively federal and state prudential regulators will examine financial institutions for compliance with the BIS guidance.

- Perhaps more than any other factor, this will impact the level of attention and resources institutions must devote to the BIS guidance.
- Notably, the guidance borrows from concepts associated with BSA compliance.
 - It incorporates BSA monitoring and reporting requirements.
 - Regulatory scrutiny of export control compliance likely will lead to scrutiny under the BSA.
 - If that happens, financial institutions can expect more pressure to strengthen export controls compliance.