Davis Polk

BIS guidance expands export control compliance expectations for financial institutions

October 21, 2024 | Client Update | 10-minute read

The Commerce Department's Bureau of Industry and Security released new guidance that, although new regulations have not been adopted, implies a significant expansion of U.S. export control compliance obligations of financial institutions. In this client update, we describe key takeaways from the guidance.

On October 9, 2024, the Bureau of Industry and Security (BIS) issued new guidance for financial institutions on best practices for compliance with export control laws and regulations (the Guidance).[1] The Guidance caps a series of notes and alerts that BIS and other regulators have released in recent years highlighting the compliance obligations of financial institutions under U.S. export control laws (as discussed in prior client updates here and here). It also follows BIS's recent final rule tightening its voluntary self-disclosure (VSD) and enforcement guidelines.[2]

As BIS stated in the Guidance, the export control compliance expectations for financial institutions "have increased significantly" in the wake of Russia's invasion of Ukraine and the expansion of national security-related trade controls targeting China. The Guidance sets out – in notably prescriptive terms – affirmative obligations for policies, procedures, and practices that BIS expects financial institutions to maintain to comply with the Export Administration Regulations (EAR). These expectations include real-time screening of transactions against lists of parties subject to export restrictions or believed to be engaged in prohibited exports and halting such transactions for investigation, as well as transaction monitoring and investigation to identify potential export control violations after the fact. Combined with BIS's new VSD policies imposing penalty enhancements for failure to disclose identified violations, the burden could be significant.

Although it remains the case that, under the law, financial institutions are only liable for "knowing" participation in U.S. export control violations, the Guidance sets out BIS's position that robust export control compliance procedures, well beyond those currently maintained by many financial institutions, are required to avoid an imputation of "knowledge" of violations of the EAR that allegedly could have been discovered. This may create challenges for many institutions arising from the volume of transactions they process, the timing of funds flows, and the limited information they generally possess about the underlying export activity. In light of the Guidance, financial institutions may need to consider enhancements to their compliance programs to meet what appears to be increased expectations that they play a role in the detection and prevention of export control violations, which (given that export controls implicate not only the identity and location of the parties, but the origin, nature, and use of any goods involved in the underlying commercial transactions and that a number of major multinational companies, particularly in China, are named on export control lists) could impose new and significant burdens on financial institutions beyond those embodied in current anti-money laundering and sanctions programs.

We provide below the key takeaways from the Guidance and the implications for financial institutions.

I. The existing focus on export control compliance appears to be expanding to bring in financial institutions.

In recent years, export control restrictions have occupied an increasingly key role in U.S. foreign and national security policy. Export controls have been central, for example, in the Biden administration's strategic response to Russia's invasion of Ukraine, and the United States continues to leverage export control laws and regulations to limit China's access to advanced technology and components, including semiconductors. The scope and complexity of export controls have expanded significantly in recent years, with BIS expanding controls on exports to Russia to include a wide variety of goods not subject to dual-use export controls, focusing on the "Common High-Priority List," and expanding restrictions on major Chinese companies, end-uses, and end-users via BIS's Entity List.

In parallel, U.S. regulators have emphasized export control compliance in a series of notices released by BIS, the Justice Department, the Financial Crimes Enforcement Network (FinCEN), and the Office of Foreign Assets Control (OFAC) since 2022.[3] In particular, two joint notices issued by BIS and FinCEN have emphasized the importance of identifying and reporting potential violations of export control laws, focusing in particular on trade finance transactions (in which financial institutions often have access to information regarding the goods being exported).[4] The Guidance is notable, however, in moving beyond trade finance, including in some cases real-time transaction screening against BIS restricted parties lists and not just after the fact reporting of suspicious activity.

II. BIS expects robust, risk-based due diligence and monitoring.

The Guidance sets out BIS's expectations for financial institutions' policies and procedures to comply with the EAR, including standards for risk-based due diligence and monitoring. The Guidance focuses, in particular, on compliance obligations under the EAR's General Prohibition 10 (GP 10),[5] which prohibits financial institutions and other persons from financing or otherwise servicing 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 and from supporting other specified activities that they know will involve certain WMD or military-intelligence programs.[6] Under GP 10, "knowledge" can be imputed on a financial institution based on "awareness of a high probability" of a violation or based on conscious disregard of facts or willful blindness. BIS states in the Guidance that this can occur when a financial institution finances or facilitates a transaction in the face of potential red flags (such as transactions involving restricted parties).

In the Guidance, BIS interprets "knowledge" under GP 10 broadly such that it places an affirmative duty on financial institutions to investigate and screen for potential violations of the EAR. While BIS acknowledged that financial institutions often have limited information about an export-related transaction, BIS expects financial institutions to implement risk-based controls into their compliance and risk management process to avoid violating GP 10. At a high level, BIS's expectations include:

- **EAR-related due diligence at onboarding.** Financial institutions should conduct due diligence on customers (and, on a risk basis, their customer's customers) at onboarding and during the course of the relationship, including screening against restricted parties lists such as Commerce's Entity List, as well as lists of entities that have shipped Common High Priority List items to Russia since 2023. On a risk basis, financial institutions should also obtain certifications from clients regarding their EAR compliance controls.
- **Ongoing transaction reviews and monitoring.** In addition to onboarding processes, BIS expects financial institutions to "review transactions on an ongoing basis for red flags." Unless an entity is on a restricted party list (described below), BIS does not expect financial institutions to review transactions in real time. However, financial institutions should maintain controls 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 (e.g., by declining further transactions). Certain red flags, such as a customer's refusal to provide requested information, may presumptively give rise to "knowledge" under GP 10 for subsequent transactions that violate the EAR.[7]
- **Real-time screening.** Although in most cases BIS does not expect financial institutions to assess every transaction for EAR compliance in real time, BIS does recommend real-time screening of customers and counterparties against BIS-administered restricted parties list when processing cross-border payments and other transactions that are likely to be associated with exports.[8] 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, but BIS does not expect financial institutions to request the names of additional parties. If there is a match to a party on one of those lists, financial institutions are expected to decline to proceed with that transaction unless the institution can determine that the transaction is authorized or permissible. A failure to do so may expose the institution to the risk of a "knowing" violation of GP 10.

III. The Guidance raises the bar for EAR compliance and may require financial institutions to update their policies and procedures.

The Guidance arguably heightens the compliance obligations of financial institutions under the EAR; while financial institutions have previously been expected to maintain procedures to manage trade finance-related risks and to report suspicious transactions related to export control evasion,[9] the Guidance articulates a more proactive role for financial institutions in monitoring for and investigating EAR violations. In effect, GP 10's prohibition on knowingly or willfully facilitating an EAR violation has shifted to an obligation to actively screen for and investigate red flags and non-compliance.

While the Guidance provides a high-level overview of BIS's expectations, it is less clear how financial institutions are expected to implement and comply with the Guidance in practice. For example, financial institutions are expected to investigate transactions for red flags post facto, which will likely be challenging for many institutions owing to the volume of transactions they process and the limited information they possess about the underlying activity (which may limit their ability to identify certain red flags in the first instance). Similarly, the Guidance would require financial institutions to stop payments on cross-border transactions involving parties on BIS-administered lists and investigate the transaction to determine if an unauthorized export has taken place, which may not be feasible for some institutions as a technical matter.

As in other areas, however, financial institutions will be expected to take a reasonable risk-based approach. In practice, this would likely require enhancements to screening procedures and policies for risk-based review and investigation. In the immediate term, some financial institutions may be required to review their compliance controls and determine if any updates are required. In any case, further guidance from BIS will be required to understand the full scope of BIS's expectations.

IV. BIS and regulators signal increased enforcement.

BIS reiterated throughout the Guidance that the failure to implement and follow appropriate compliance controls creates the risk of a violation under GP 10. The Guidance also encouraged voluntary self-disclosure of internally identified violations. In this regard, the Guidance aligns with recent public statements and guidance from the DOJ and regulators, which signaled an intent to take an aggressive enforcement posture for export control violations and encouraged proactive disclosure.

The BIS underscored this focus on enforcement last month through a final rule that codified prior memoranda and meaningfully sharpened the EAR's VSD and penalty provisions. Among other things, the final rule amended the factors used to determine BIS's administrative response to a violation such that a person's deliberate decision not to disclose a violation will be treated as an aggravating factor in BIS's enforcement decision-making and subsequent administrative penalties. The final rule also updated BIS's penalty guidelines to allow for more substantial penalties in high-value transactions. We expect that BIS's proactive enforcement posture, and its heightened compliance expectations for financial institutions, will continue for the foreseeable future.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Kendall Howell
+1 202 962 7068
kendall.howell@davispolk.com

Paul Marquardt
+1 202 962 7156
paul.marquardt@davispolk.com

Will Schisa
+1 202 962 7129
will.schisa@davispolk.com

Daniel P. Stipano
+1 202 962 7012
dan.stipano@davispolk.com

Charles Marshall Wilson
+1 202 962 7130
charles.wilson@davispolk.com

1 BIS, Bureau of Industry and Security Issues New Guidance to Financial Institutions on Best Practices for Compliance with the Export Administration Regulations (October 9, 2024), https://www.bis.gov/media/documents/guidance-financial-institutions-best-practices-compliance-export-administration.

2 89 Fed. Reg. 45477 (Sep. 16, 2024).

3 *See, e.g.,* BIS, Russia Evasion Tactics: Red Flag Indicators, *available at*: https://www.bis.gov/sites/default/files/files/RedFlags.pdf; BIS, Guidance to Prevent Evasion of Prioritized Harmonized System Codes to Russia (May 19, 2023), https://www.bis.doc.gov/index.php/documents/enforcement/3278-bis-guidance-to-prevent-evasion-of-prioritized-harmonized-system-codes-to-russia-final/file; Department of Commerce, Department of the Treasury, and Department of Justice, Tri-Seal Compliance Note: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls (March 2, 2023), https://ofac.treasury.gov/media/931471/download?inline; Department of Commerce, Department of the Treasury, Department of State, and Department of Justice, Guidance to Industry on Iran's UAV-Related Activities (June 9, 2023), https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3286-quad-seal-advisory/file; FinCEN and BIS, FIN-2023-Alert004, Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts (May 19, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN%20and%20BIS%20Joint%20Alert%20_FINAL_508C.pdf; FinCEN and BIS, FIN-2022-Alert003, FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts (June 28, 2022), https://www.fincen.gov/sites/default/files/shared/FinCEN%20and%20BIS%20Joint%20Alert%20FINAL.pdf.

4 *See id*.; FinCEN and BIS, FIN-2022-Alert003, Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts.

5 15 C.F.R. § 736.2.

6 *Id.*

7 Other red flags include a party's "match" on a restricted party list, transactions involving companies that share a location with a sanctioned entity or a company on the Entity List, and transactions involving a last-minute change in payment routing that was previously scheduled from a country

of concern. Financial institutions can resolve these red flags by, among other things, confirming that the underlying export was licensed.

[8] The Guidance notes in particular that financial institutions should screen against the Denied Persons List, the military-intelligence end users identified in 15 CFR § 744.22(f)(2), and some (but not all) parties on the Entity List.

[9] *See, e.g.*, FinCEN and BIS, FIN-2022-Alert003, FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts.