STEPTOE OUTSIDE COUNSEL

Updated guidance on potential Russian export control evasion

The US Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") and the US Department of Commerce's Bureau of Industry and Security ("BIS") have issued a supplemental joint alert ("Supplemental Alert") regarding efforts by parties to evade US export controls implemented after Russia's invasion of Ukraine.[1] The alert provides helpful information for exporters in the 39 nations of the Global Export Control Coalition ("GECC") regarding compliance initiatives to stop Russia procuring goods and technology in support of harmful military activities.

Building off a joint alert issued in 2022,[2] the Supplemental Alert provides updated guidance to assist financial institutions in identifying suspicious financial transactions relating to possible export control evasion. Even if you are not a financial institution, this guidance is still relevant. GECC exporters should be mindful that enhanced compliance program systems, processes, and efforts may be necessary or prudent to implement in order to ascertain indicators of evasive activity.

The Supplemental Alert identifies nine Harmonized System ("HS") codes regarding critical US components that Russia relies on for its weapons systems that have been recovered on the battlefield in Ukraine, including electronic integrated circuits, radio navigational aids, capacitors, wireless transceiver modules, and other electrical parts. This is not an exhaustive list, but it provides specific HS codes for items that the US government has assessed that Russia is using evasive methods to acquire. Importantly, the EU, UK, and Japan have partnered with FinCEN and BIS concerning this diversion risk assessment, so even if items are not US-origin, exporters in those jurisdictions also should be mindful of evasion concerns regarding them.

Additionally, the Supplemental Alert encourages financial institutions to review information on commercial documentation when encountering one of the nine listed HS codes to identify possible third-party intermediaries and attempts at evasion of US export controls. In reviewing US export data related to these nine HS codes, certain fact patterns associated with importers in non-GECC countries raised diversion or transshipment concerns to Russia, such as where a company:

- never received exports before 24 February 2022;
- received exports that did not include any of the nine HS Codes before 24 February 2022; or
- received exports involving the nine HS Codes before 24 February 2022, but then significantly increased orders afterward.

Where identified, financial institutions are urged to conduct due diligence, such as evaluating

- the customer's date of incorporation (e.g., after 24 February 2022);
- the end-user and end use of the item (e.g., whether the customer's line of business is consistent with the ordered items);
- whether the customer's physical location and public-facing website raise any red flags; and
- anomalous increases in the volume or value of orders (e.g., customer is overpaying), or inconsistencies between the items ordered and customer's line of business.

A notable activity is disguising the involvement of persons on the US Office of Foreign Assets Control's SDN List or BIS Entity List to obscure the true identities of Russian end-users. A common tactic involves the use of front (shell) companies outside Russia.

If financial institutions engaged in providing financial transactions analyze such information and are required to submit suspicious activity reports to government authorities, then exporters should consider such potential red flag indicators of export control evasion that may be reported, where warranted, stop transactions of concern, and implement a risk-based export control and sanctions compliance program to comply with applicable law. In that way, exporters will be better positioned to prevent violations, mitigate the possibility of investigations by the US government, or address requests for information from financial institutions undertaking transactions on behalf of exporters. ■

About the authors:

Jack Hayes is Of Counsel in the Washington, DC office of Steptoe.

www.steptoe.com

[1] Supplemental Alert: FinCEN and BIS Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts, FIN-2023-Alert004 (19 May 2023) at https://www.fincen.gov/sites/default/files/shared/FinCEN%20and%20BIS%20Joint%20Alert%20_FINAL_508C.pdf.

[2] FIN-2022-Alert003 (28 June 2022) at https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf.

Procurement agents arrange purchases of goods by the company from various suppliers, who in turn receive payment from the front company's non-Russian bank account, which may transmit funds through a correspondent bank account to pay the supplier. The front company will then route the goods to Russia, often through transshipment jurisdictions.