



FOR IMMEDIATE RELEASE

July 10, 2024

www.bis.gov

BUREAU OF INDUSTRY AND SECURITY

Office of Congressional and Public Affairs

Media Contact: OCPA@bis.doc.gov

BIS Issues Guidance on Addressing Export Diversion Risks

WASHINGTON, D.C. – Today, the Department of Commerce’s Bureau of Industry and Security (BIS) [published guidance](#) outlining the different actions that BIS takes to inform industry and academia about parties – beyond those identified on public screening lists like the Entity List – that present risks of diversion of items subject to BIS export controls to countries or entities of concern. The guidance also outlines certain responsibilities companies and universities have to comply with BIS regulations, as well as additional steps they should take to mitigate diversion risks.

“Partnering with industry and academia to identify diversion risks is a cornerstone of our enforcement strategy to safeguard U.S. exports,” said **Assistant Secretary for Export Enforcement Matthew S. Axelrod**. “By sharing information in these different ways – from supplier lists made available by BIS or the Trade Integrity Project, to parties identified in ‘red flag’ letters or ‘is informed’ letters, to persons identified on the Entity List – we are helping U.S. exporters to better screen their customers and protect U.S. national security.”

Today’s guidance also contains a new recommended best practice asking that exporters, reexporters, and transferors of Common High Priority List (CHPL) items screen transaction parties using online resources made newly available by the [Trade Integrity Project](#) (TIP). Specifically, the TIP identifies third-country suppliers with a history of exporting CHPL items to Russia since its full-scale invasion of Ukraine. The TIP screening tool can enable companies and universities around the globe to identify possible red flags prior to proceeding with an export transaction that risks diversion to Russia.

BIS generally administers controls on end users by designating them on one of its public screening lists – e.g., the Unverified List, Entity List, Military End-User List, and Denied Persons List – each of which imposes its own specific set of requirements under the Export Administration Regulations (EAR) involving listed parties. BIS uses a variety of additional mechanisms to alert or notify companies or universities about other parties of national security concern, such as those that present a risk of diverting EAR items to restricted end uses or end users in Russia. These mechanisms are “Supplier List” letters, Project Guardian Requests (where BIS asks companies and universities to be on the lookout for specific transactions and take certain actions), Red Flag Letters, and “Is Informed” letters. The guidance document issued today, which can be found [here](#), explains these different mechanisms and identifies associated due-diligence responsibilities and best practices under the EAR.

Since February 24, 2022, BIS has implemented a series of [stringent export controls](#) that restrict Russia's access to the technologies and other items that it needs to sustain its brutal war against Ukraine. These restrictions also apply to Belarus in response to its substantial enabling of Russia's destabilizing conduct.

For more information, visit: www.bis.gov.