Middlebury Institute *of* International Studies at Monterey
James Martin Center for Nonproliferation Studies

Export Control Red Flags with Russia and China

Sept 2022

This document is intended to be a starting point for identifying red flags for suspicious transactions, with an emphasis on concerns surrounding emerging technologies. While this list attempts to be comprehensive, it should not be considered a checklist for due diligence. For more information on strategies to counter risk and on how academic research has informed the identification of these red flags, please visit our website at www.tradecompliance.io.

Entity Specific Red Flags

Company/Partner	Academic Involvement	Illicit Involvement
• Company is linked to the military or on a watch list • Company operates in a strategic sector • Company's website identifies problematic activity such as links to military end-uses and/or military end-users of concern • Company is less than 5 years old • Company has previous negative publicity for proliferation concerns • Company is an authorized arms manufacturer or is listed as a strategic enterprise • Company's website has a communist party page demonstrating its close links to the Chinese state.	• Entity is a university in a country of concern (or identified explicitly on a sanctions/restricted party list or on the ASPI University tracker • Entity has an academic program or laboratory in a strategic field and receives government sponsorship • Entity has a known linkage to national laboratory researchers in a strategic field	• Is there a lack of information on end use? Is the procurer an intermediary rather than an end user? Are they hesitant to provide information on the actual end user? • Lack of company website or other official presence • Cash payments for expensive orders that usually are financed • Incomplete orders, shipments for specific parts

Transaction Specific Red Flags

Company/Partner	Academic Involvement	Illicit Involvement
• Company is linked to the military or on a watch list • Company operates in a strategic sector • Company's website identifies problematic activity such as links to military end-uses and/or military end-users of concern • Company is less than 5 years old • Company has previous negative publicity for proliferation concerns • Company is an authorized arms manufacturer or is listed as a strategic enterprise • Company's website has a communist party page demonstrating its close links to the Chinese state.	• Entity is a university in a country of concern (or identified explicitly on a sanctions/restricted party list or on the ASPI University tracker • Entity has an academic program or laboratory in a strategic field and receives government sponsorship • Entity has a known linkage to national laboratory researchers in a strategic field.	• Is there a lack of information on end use? Is the procurer an intermediary rather than an end user? Are they hesitant to provide information on the actual end user? • Lack of company website or other official presence • Cash payments for expensive orders that usually are financed • Incomplete orders, shipments for specific parts

Technology Specific Red Flags

- Is the technology on a control list?
- Is the technology a chokepoint technology?
- Is the technology sought by a country of concern through a nationalized indigenization plan?
- Was a military-grade product sought for civilian purposes when a civilian-grade option is available?
- Does the technology feature in the sectoral analysis section of this guidance?

Country Specific Red Flags

Russia	China
• Is the company a wholesaler? Wholesalers are often used as intermediaries by Russian companies engaged in emerging technology development to access parts and components. • Does your business partner in your country own a company inside of Russia? This is a common technique in more sophisticated procurement attempts. • Is the company attempting to buy electronics, machine tools or other goods that can be used in armaments production? • Is the company asking you to pay via cryptocurrency or to a bank account in a third country? • Does the company have a website? Does the website advertise that they can help their customers avoid trade restrictions?	• Company has a known link to the Thousand Talents Plan or similar recruitment agencies. • Company is in a strategic industry and located in a domestic geographical hub near other entities in that industry. • Is the end user one of the authorized military goods manufacturers or is it a strategic entity such as CASC, China Academy of Launch Vehicle Technology, or the Chinese Academy of Engineering Physics?

Resources to Reference

When assessing red flags, there are several resources and reference materials available to provide additional insight into the entities being investigated. The following is a list of common reference materials and sources compliance officers should be checking when performing due diligence assessments. This list is meant to be a starting point but not a checklist on due diligence resources.

- LinkedIn or other social media presence for the entity
- News media coverage
- Sanctioned entity lists (namely the China country section of the US BIS Entity List and the DOD ''Chinese Military Companies List' per Section 1260H of the NDAA of 2021; and the U.S. Treasury Dept. OFAC's "Non-SDN Chinese Military-Industrial Complex Company List (NS-CMIC List)
- Foreign End-User Lists
- ASPI University Tracker
- University/Institute websites, including sources of funding and awards/recognitions received
- Controlled Technology Lists

CNS Sectoral Guidance

These red flags are an extract from the CNS sectoral guidance on export controls in an era of strategic competition. To read the full guidance, including the due dilligence guidance which complements these red flags, visit www.tradecompliance.io.