REPRINT

R&C risk & compliance

EXPORT COMPLIANCE AND ENFORCEMENT

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JUL-AUG 2023 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

BDO

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

www.riskandcompliancemagazine.com

ONE-ON-ONE INTERVIEW

EXPORT COMPLIANCE AND ENFORCEMENT

Richard Weinert
Director, Legal Monitorships & Investigations
BDO USA, LLP
T: +1 (212) 885 7453
E: rweinert@bdo.com

Richard Weinert is a director in BDO's forensics practice with more than 15 years of experience providing forensic accounting, advisory and compliance related services. He helps private and public companies build and maintain effective export compliance programmes and is responsible for leading export compliance risk assessments, conducting export compliance audits, and developing and implementing corrective actions in response to internal control weaknesses.

R&C: Could you provide an overview of the key global trends impacting the trade landscape and the obligations of exporters? What issues are adding to an already complex area?

Weinert: In the wake of the Russia-Ukraine conflict and the ongoing 'chip war', companies are re-evaluating their supply chains and assessing the potential impact of additional sanctions and export controls across their networks. In particular, we are starting to see companies that deal with sensitive technologies move operations out of China into other Asian nations. At every step of the supply chain, companies are scrutinising their business partners. This can help mitigate potential violations of the US Export Administration Regulations (EAR) and address reputational risks. For example, a drone manufacturer found that its products had appeared on the Ukrainian battlefield. The drones had likely gone through intermediaries, emphasising the importance of knowing not only the customer but also the customer's customer and ultimate end-users.

R&C: What do you consider to be the most significant regulatory changes to have impacted export compliance in recent months? How have exporters responded?

Weinert: In response to the Russia-Ukraine conflict, numerous countries have implemented export controls. Companies must now navigate a complex jurisdictional maze of regulation. For example, the definition of 'control' of an entity may vary by country or jurisdiction. As a result, companies have had to revisit the lists against which they screen their customers and business partners. They must also conduct enhanced due diligence on certain relationships. We are also observing greater coordination across sanctions regimes and countries. With respect to export controls, this is the first time we have seen such a multilateral approach across the US, European Union (EU) and other nations to deprive Russia and China of military technology and equipment. In October 2022, the Bureau of Industry and Security (BIS) implemented additional controls on China with respect to advanced computing semiconductors and supercomputers, limiting China's ability to produce advanced weapons systems.

R&C: What kinds of fines, penalties and reputational harm might befall companies that fail to meet their export compliance requirements?

Weinert: BIS, which has been active with its enforcement actions, has multiple levers it can pull, including adding entities to the entity list, military end

user (MEU) list or issuing denial orders to companies that violate the EAR. In 2022, BIS also announced enforcement changes, including higher penalties for more serious violations and a process to expedite less serious or technical ones. We are also seeing increases in fines and penalties. In April 2023, a large multinational company was fined $3.3m for alleged violations of export controls and sanctions. BIS recently imposed a $300m civil penalty, the largest standalone penalty in its history, to resolve alleged violations of the EAR. Fines and penalties can have a substantial impact on a company's reputation. For example, if a company is selling sensitive technologies that end up in embargoed countries, other organisations or consumers may refuse to do business with them.

> **"At every step of the supply chain, companies are scrutinising their business partners."**
>
> *Richard Weinert, BDO USA, LLP*

R&C: Amid ramped-up enforcement activity, what advice would you offer to companies on reviewing their internal export compliance procedures?

Weinert: First, companies should assess their export control compliance risks and employ a risk-based approach to their export control compliance programmes. Certain products, customers and geographies will have higher or lower export compliance risk, which should be factored into the export control compliance programme. Companies should focus their limited resources where they can have the greatest impact on mitigating export control risks and potential violations. Second, companies should ensure they have well-documented export control processes and procedures with clearly defined roles, responsibilities, escalation and reporting protocols. Companies should periodically audit and self-check their internal controls and record-keeping practices to determine whether policies are being followed and internal controls are being executed and operating effectively.

R&C: How can exporters go about verifying their customers and end users to ensure products and technologies are

not exported to restricted entities or destinations?

Weinert: Exporters must use the information they collect from customers, as well as publicly available information, to verify customers' representations. For example, geolocation information on shipments can validate end-users and destinations. Companies should also have a risk-based know your customer (KYC) programme that outlines the specific information that must be documented, as well as the appropriate resources to consult. Exporters should make sure they understand the products they are selling, whether such items are subject to the EAR and the proper export control classification numbers for those items. This will determine to whom and where those products may be sold. Finally, companies should include audit rights in their sales contracts. These audits allow companies to periodically conduct risk-based audits or inspections to validate the end-user representations made by their customers and distributors. Activating such audit rights may uncover important information on the ultimate end-users or highlight needed enhancements to existing due diligence procedures.

R&C: To what extent are companies using technology to automate time-consuming processes and help ease the burden of export compliance?

Weinert: There are several areas where companies are using technology to streamline their operations. Numerous tools and software programmes can help companies with the screening process, including automated continuous screening software and subscriptions for consolidated screening entity and sanctioned party lists. Companies can also make use of public records resources and subscriptions when performing due diligence, helping to ease the burden of export compliance. When using screening software, companies can fine-tune and optimise algorithms and parameters to reduce the number of screening alerts and false positives. Furthermore, companies are increasingly looking at artificial intelligence and robotic process automation to streamline the alert management and clearance process.

R&C: What developments do you expect to see in the export compliance and enforcement space over the months and years ahead? In your experience, are exporters doing enough to prepare their operations for the future?

Weinert: We expect to see current trends continue, with enforcement focused on actors that threaten national security. We expect BIS to add entities to the entity list, particularly those involving advanced technology or with military ties

in Russia or China. We also expect to see greater coordination across agencies and jurisdictions. For example, the Department of Justice and Department of Commerce recently announced the launch of the Disruptive Technology Strike Force to protect critical US technology from getting into the wrong hands. Many companies view the Russia-Ukraine conflict and increased enforcement actions as an opportunity to strengthen their compliance programmes. Within these organisations, we have seen increased investment in human capital and information technology to support export controls. As the regulatory landscape evolves, companies must be ready to pivot from their normal course of business, resulting in potential changes to their supply chain, sales distribution channels and business partners. R&C