KPMG

China Tax Alert

Issue 14, August 2023

U.S. BIS, OFAC and DOJ jointly issue a compliance note on voluntary self-disclosure

Summary：

- A Compliance Note was released on July 26, 2023, by the U.S. Department of Commerce's Bureau of Industry and Security (BIS), the Department of Treasury's Office of Foreign Assets Control (OFAC), and the Department of Justice's National Security Division (NSD). The Note summarizes the process of voluntary self-disclosure (VSD) by companies for potential violations relating to export controls and sanctions that may affect national security. It emphasizes that VSD can reduce administrative or criminal liability for violations and also helps the relevant national security agencies respond to threats to U.S. national security.
- The Note provides information on the guidelines and benefits of VSD for companies under BIS, OFAC and NSD. It explains how VSD can be considered qualified, the importance of cooperation with enforcement authorities and how it can help mitigate the consequences of a breach. BIS policy on VSD also covers the requirements and incentives for companies to report potential violations by third parties. The VSD policies of all three agencies emphasize the effectiveness of a company's Internal Compliance Program (ICP) in addressing and resolving any potential breaches in a prompt manner.

Background

In recent years, the U.S. government has increasingly prioritized national security in domestic and foreign policy. Export controls and sanctions have been implemented to protect national security, with a particular emphasis on promoting corporate compliance and enforcement. The Compliance Note emphasizes companies' critical role in maintaining national security by complying with export controls, sanctions, and other national security-related laws. The U.S. government relies on cooperation from companies to prevent adversaries' use of U.S. technologies and financial systems and safeguard national security. As a result, BIS, OFAC, and NSD have updated their VSD policies to encourage proactive compliance and facilitate regulation and enforcement by government agencies. This promotes the effective implementation of U.S. export controls and sanctions policies.

The Export Administration Regulations (EAR) include BIS's policy on VSD for export control violations. BIS has adopted a "dual-track" approach at the enforcement level, where potential breaches voluntarily disclosed by companies are categorized based on their severity. Minor infringements are dealt with promptly and generally without significant enforcement action or penalties, while more severe breaches are investigated by specially assigned personnel. BIS's enforcement process is designed to encourage businesses to voluntarily disclose violations, while prioritizing government resources on more serious breaches. Deliberate non-disclosure of potential breaches will be considered an aggravating factor. A company's voluntary disclosure or a third party's report of a breach will be regarded as a mitigating factor in BIS's treatment of a company's breach, even if the two violations are unrelated.

When it comes to penalties for violating sanctions, OFAC's VSD Policy takes into account voluntary disclosures as a mitigating factor. If disclosure is qualified, it can lower the liability by as much as 50%. Additionally, FinCEN, which OFAC heads, encourages third parties to report economic sanctions violations and may offer cash rewards to whistle-blowers.

The NSD, a branch of the US Department of Justice that handles national security violations such as export controls and economic sanctions, has recently updated a VSD policy focusing on criminal violations in these areas. This policy differs slightly from that of BIS or OFAC. As a specialized legal agency, NSD has more detailed VSD requirements than BIS and OFAC, with stricter criteria for determining a qualified VSD. Companies that voluntarily disclose their potential criminal offenses to NSD, cooperate fully, take correct and timely remedial action, and have no other aggravating factors, may be able to obtain a non-prosecution agreement and pay no fines.

KPMG observations

The Note and statements from three agencies clarify the US government's stance on corporate compliance regarding export controls and economic sanctions. Companies are crucial in achieving national security policy goals and are urged to cooperate with government agencies in proactive compliance. Intentionally concealing violations will result in severe punishment. Companies that may be impacted by US regulation should adopt a proactive approach to compliance issues in response to regulatory trends by US government agencies.

BIS, OFAC, and NSD stress the importance of a company's ICP and its response to potential breaches when assessing its VSD. To show regulators that a company has carried out its compliance duties well and to help seek the best possible outcome in the event of a breach, it is crucial to establish and implement a comprehensive ICP that meets the requirements set by the relevant regulatory bodies. Maintaining accurate records is also essential.

In the process of VSD, different government agencies have unique requirements at both the practical and procedural levels. If a company suspects a violation, it must first identify the appropriate authority and prepare the necessary materials per the relevant procedures. The company must then submit these materials within the specified timeframe. It's worth noting that if multiple competent authorities are involved, a VSD to one authority does not guarantee acceptance by the other authorities. Furthermore, for a VSD to be considered voluntary disclosure by the company, it must be explicitly authorized by the management.

Chinese companies considering VSD must ensure compliance with relevant Chinese laws and regulations. Data and privacy security laws require companies in China to abide by applicable outbound data regulations when providing information overseas, particularly to foreign government agencies. Anti-foreign sanctions and blocking laws also impose restrictions on the activities of companies in China under certain foreign sanctions. Meanwhile, newly revised anti-espionage laws and regulations mandate new national security compliance requirements on companies that provide information overseas. Additionally, China's Ministry of Commerce and other authorities require companies to report to and obtain prior approval before accepting investigations by foreign governments.

If you have any questions about the above contents, please contact the relevant tax experts of KPMG and have an in-depth discussion.

kpmg.com/cn/socialmedia

For more information of KPMG China tax services, please scan the QR code or visit our website:
https://kpmg.com/cn/en/home/insights/2023/01/china-tax-alert.html

For a list of KPMG China offices, please scan the QR code or visit our website:
https://home.kpmg.com/cn/en/home/about/offices.html