US GOVERNMENT TO PENALIZE FAILURES TO DISCLOSE POSSIBLE EXPORT CONTROL VIOLATIONS AND INCENTIVIZE REPORTING OF OTHERS' VIOLATIONS

Date: 2 May 2023

US Policy and Regulatory Alert

By: Guillermo S. Christensen, Anna E. L'Hommedieu, David C. Rybicki

A common approach in dealing with potential violations of the US export control laws is to undertake a voluntary disclosure to the regulators and thereby benefit from long-standing policies that favor such disclosure by reducing penalties—in essence prioritizing a partnership between the government and companies to improve compliance with export controls. The Office of Export Enforcement (OEE) of the US Department of Commerce, Bureau of Industry and Security (BIS), recently announced that it will pursue a harder line on potential violations that are not self-disclosed, threatening companies that decide against such disclosures with aggravated punishment.

AGGRAVATED PUNISHMENTS FOR COMPANIES WHO FAIL TO SELF-DISCLOSE VIOLATIONS

The Department of Commerce recently disclosed an 18 April internal memorandum from Matthew Axelrod, the Assistant Secretary for Export Enforcement (the Memo), directing export enforcement personnel to pursue increased penalties against companies that fail to file a voluntary self-disclosure (VSD) after a party uncovers "significant" possible violations of the Export Administration Regulations (EAR).[1] The Memo does not clarify what constitutes a "significant" violation, but notes that such violations "reflect potential national security harm" and are more than minor technical violations.

Administered by BIS, the EAR impose, among other restrictions, controls on the export, re-export, transfer, or other release of various items that fall within the scope of EAR jurisdiction, including "dual use" commodities, software, and technology (i.e., items that may serve both commercial and military functions). A primary purpose of these controls is to inhibit adversaries abroad from obtaining EAR items that they may use for malign purposes.

The Memo signals a significant shift in BIS enforcement policy, as previously companies that filed VSDs could receive partial or total mitigation of civil penalties, but were not penalized if they failed to voluntarily come forward. The Memo notes that the purpose of the policy shift is to further incentivize the submission of VSDs when industry or academia uncovers significant possible violations of the EAR and that "when someone affirmatively chooses not to file a VSD . . . they risk incurring concrete costs."

In explaining this policy shift, the Memo notes that this approach is consistent with the existing BIS penalty determination guidelines. In particular, the guidelines require consideration of "whether a Respondent's export

©2005-2026 K&L Gates LLP. All Rights Reserved.

compliance program uncovered a problem, thereby preventing further violations, and whether the Respondent has taken steps to address compliance concerns raised by the violation, to include the submission of a VSD and steps to prevent reoccurrence of the violation that are reasonably calculated to be effective."[2] The Memo notes that this is a "General Factor" that is designed to be "either mitigating or aggravating." Under the prior policy, submission of a VSD could only be considered a mitigating factor. Under the new policy, submission of (or failure to submit) a VSD can be either a mitigating or an aggravating factor. Importantly, OEE will now "consistently apply this factor as an aggravating factor when a significant possible violation has been uncovered by a party's export compliance program but no VSD has been submitted."

Accordingly, companies should carefully weigh any decision not to disclose significant possible violations and will "benefit greatly by getting a sharply reduced penalty" by filing a VSD. Companies will have to grapple with the severity of their possible violations, particularly in light of the ambiguity surrounding what constitutes a "significant" violation and potential exposure to criminal liability that disclosure of such violations might entail.

This policy change is in line with the government's increasing focus on the critical nature of US dual use export controls to US national security. Historically, such policies had already been in place for items or information subject to the most significant controls (e.g., military items).[3] This trend towards stricter control of dual use items is also being demonstrated by recent export control enforcement actions. For example, BIS recently imposed a US$300 million penalty in April 2023 against Seagate Technology LLC of Fremont, California and Seagate Singapore International Headquarters Pte. Ltd. of Singapore for sales of hard disk drives to affiliates of Huawei, the Chinese telecommunications multinational company that is a primary focus of US export control and government contract restrictions.[4] This penalty represents the largest standalone administrative penalty in BIS history. The Department of Justice (DOJ) also recently announced that it will add 25 new prosecutors to focus on counter intelligence and export controls, which is likely to increase the enforcement actions in the export controls area.[5]

INCREASED INCENTIVES FOR WHISTLEBLOWERS

The Memo also highlighted a second critical compliance area that will incentivize whistleblowers to report companies that violate export rules. The EAR contains a provision that allows for the reporting of others' violations.[6] The Memo noted that in the settlement guidelines, the OEE will consider "previously made substantial voluntary efforts to provide information (such as providing tips that led to law enforcement actions against other parties) to federal law enforcement authorities in support of the enforcing of U.S. export control regulations." This would essentially allow a company to "bank" mitigating factor credit in the event that it ever faces future enforcement action.

Not only can reporting be used for mitigating credit with the OEE, but also companies and individuals may receive monetary awards for disclosing possible export control violations that involve potential sanctions violations. The Financial Crimes Enforcement Network (FinCEN) has a whistleblower program that provides substantial financial awards if information a whistleblower provides to FinCEN or the DOJ about violations of US sanctions programs and the Bank Secrecy Act results in a successful enforcement action. FinCEN can pay awards to whistleblowers whose information leads to successful "related actions," including EAR violations.

©2005-2026 K&L Gates LLP. All Rights Reserved.

As a result, there will likely be an increase in the confidential reporting of export control violations of other companies, and possibly increased use of the confidential reporting channel by competitors to spotlight conduct they have uncovered during routine business dealings.

CONCLUSION

In light of this announcement, it will be crucial for companies that have identified potential export control issues to review carefully these concerns to determine whether there is a path to voluntary disclosure. It is critical for companies to conduct this review and make this determination as soon as possible, so that the initiation of a government investigation does not foreclose the opportunity to file a voluntary disclosure. Equally important is that companies put in place strong compliance and risk assessment approaches that will identify potential violations early enough to allow for an assessment and action—a voluntary disclosure is typically only feasible when the company initiates the disclosure, which may not be possible if the allegation becomes known to the government through other channels.

Lawyers in the K&L Gates US National Security Law and Policy; Investigations, Enforcement, and White Collar; and International Trade groups have experience in matters involving national security, trade regulatory agencies, and DOJ investigations and enforcement actions. They are well versed in assessing export control issues when they arise and determining if voluntary disclosure or other steps are merited.

FOOTNOTES

[1] Axelrod, M., Memorandum for All Export Enforcement Employees, dated Apr. 18, 2023, https://www.bis.doc.gov/index.php/documents/enforcement/3262-vsd-policy-memo-04-18-2023/file

[2] Section III.E to Supplemental No. 1 to Part 766 of the EAR.

[3] *See, e.g.*, 22 C.F.R. § 126.1 (imposing a "duty to notify" in the case of defense article exports to certain restricted destinations).

[4] Press Release, BIS Imposes $300 Million Penalty Against Seagate Technology LLC Related to Shipments to Huawei, dated Apr. 19, 2023, https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3264-2023-04-19-bis-press-release-seagate-settlement/file

[5] Monaco, L., Deputy Attorney General Lisa Monaco Delivers Remarks at American Bar Association National Institute on White Collar Crime, dated Mar. 2, 2023, https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-monaco-delivers-remarks-american-bar-association-national

[6] 15 C.F.R § 764.4.

©2005-2026 K&L Gates LLP. All Rights Reserved.

KEY CONTACTS



GUILLERMO S. CHRISTENSEN
PARTNER

WASHINGTON, DC
+1.202.778.9095
GUILLERMO.CHRISTENSEN@KLGATES.COM



ANNA E. L'HOMMEDIEU
ASSOCIATE

BOSTON
+1.617.951.9144
ANNA.LHOMMEDIEU@KLGATES.COM



DAVID C. RYBICKI
PARTNER

WASHINGTON, DC
+1.202.778.9370
DAVID.RYBICKI@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.