Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note:

Voluntary Self-Disclosure of Potential Violations

OVERVIEW

U.S. businesses are at the vanguard of technological advancements: inventing new materials, making scientific breakthroughs, and otherwise advancing U.S. technological and financial leadership.[1] As key participants in international trade and finance, businesses also play a critical role in identifying threats from malicious actors and helping to protect our national security by complying with U.S. sanctions, export controls, and other national security laws. It is critical that businesses work together with the U.S. Government to prevent sensitive U.S. technologies and goods from being used by our adversaries and to prevent abuse of the U.S. financial system by sanctioned individuals, entities, and jurisdictions.

Compliance with sanctions, export controls, and other national security laws is paramount. If a company discovers a potential violation, whether it is an administrative or criminal violation, that company should promptly disclose and remediate. This is especially true for potential violations of U.S. national security laws, including those governing sanctions and export controls. Self-disclosing potential violations can provide significant mitigation of civil or criminal liability, the extent of which depends on the agency, but may extend so far as a non-prosecution agreement or a reduction of 50 percent in the base penalty amount for civil or criminal penalties.

To assist the private sector in ensuring that businesses and other organizations timely and appropriately disclose potential violations, this Note describes voluntary self-disclosure (VSD) policies that apply to U.S. sanctions, export controls, and other national security laws as well as recent updates that have been made to certain of those policies.

[1] *See, e.g.*, Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit (Sept. 16, 2022), available at: https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/.

Date: July 26, 2023

DEPARTMENT OF JUSTICE'S NATIONAL SECURITY DIVISION'S UPDATED VOLUNTARY SELF-DISCLOSURE POLICY

The Department of Justice's National Security Division (NSD) has long recognized that the unlawful export of sensitive commodities, technologies, and services poses a serious threat to the national security of the United States. Engaging in transactions with sanctioned individuals and entities poses an equally serious threat.

As part of its effort to address these threats, NSD on March 1, 2023, issued an updated VSD policy covering potential criminal violations of export control and sanctions laws.[2] NSD's policy is designed to provide incentives for companies and other organizations to come forward promptly when they identify or otherwise become aware of potential criminal violations of U.S. sanctions and export control laws. A prompt voluntary self-disclosure provides a means for a company to reduce—and, in some cases, avoid altogether—the potential for criminal liability.

Moving forward, where a company voluntarily self-discloses potentially criminal violations, fully cooperates, and timely and appropriately remediates the violations, NSD generally will not seek a guilty plea, and there will be a presumption that the company will receive a non-prosecution agreement and will not pay a fine. Companies that qualify for a non-prosecution agreement (or declination, where appropriate) are not permitted to retain any of the unlawfully obtained gain from the underlying misconduct. The presumption in favor of a non-prosecution agreement does not apply, however, where there are aggravating factors. Those factors include egregious or pervasive criminal misconduct within the company, concealment or involvement by upper management, repeated administrative and/or criminal violations of national security laws, the export of items that are particularly sensitive or to end users of heightened concern, and a significant profit to the company from the misconduct. Where such aggravating factors are present, NSD has the discretion to seek a different resolution, such as a deferred prosecution agreement or guilty plea.[3]

To avail itself of NSD's policy, a company must disclose to NSD within a reasonably prompt time after becoming aware of the potential violation, absent any other legal obligation to disclose, and prior to an imminent threat of disclosure or government investigation. Disclosures made only to regulatory agencies such as OFAC or BIS do not qualify for NSD's policy. The disclosing party must share with NSD all relevant non-privileged facts known at the time. In addition, a company must fully cooperate with NSD when making its disclosure. Pursuant to the updated policy, full cooperation means, among other things, timely preservation and collection of relevant documents and information, including concurrent authentication of records under Federal Rule of Evidence 902 and/or 803; deconfliction of witness interviews and other

[2] U.S. Department of Justice, "NSD Enforcement Policy for Business Organizations," (March 1, 2023), *available at* https://www.justice.gov/media/1285121/dl?inline=.

[3] *Id*. at 2.

investigative steps that a company intends to take as part of its own internal investigation; and timely identification of opportunities for further investigation by NSD.[4]

To receive the benefits from disclosure, a disclosing company must timely and appropriately remediate any violations. As part of its analysis, NSD will consider whether a company has implemented an effective and sufficiently resourced compliance and ethics program. NSD also now examines whether a disclosing company has imposed appropriate disciplinary measures, including compensation clawbacks, for employees who directly participated in or had oversight and/or supervisory authority over the area where the criminal conduct occurred.[5]

Importantly, the principles of NSD's policy also apply to other corporate criminal matters handled by NSD. Examples of such matters include those arising under the Foreign Agents Registration Act, laws prohibiting material support to terrorists, and potential criminal violations in connection with the Committee on Foreign Investment in the United States and other national security proceedings.[6] NSD has further strengthened its focus on corporate compliance with national security laws by hiring a Chief Counsel for Corporate Enforcement and by adding twenty-five new prosecutors to help investigate and prosecute sanctions evasion, export control violations, and similar economic crimes.[7]

DEPARTMENT OF COMMERCE'S BUREAU OF INDUSTRY AND SECURITY'S UPDATED GUIDANCE FOR VOLUNTARY SELF-DISCLOSURES

The Bureau of Industry and Security (BIS) strongly encourages disclosures by companies and other entities who believe that they may have violated the Export Administration Regulations (EAR), or any order, license, or authorization issued thereunder. In general, information about the VSD policy can be found in Section 764.5 of the EAR and on the Export Enforcement website.[8] A disclosure that is timely and comprehensive and involves full cooperation of the disclosing party substantially reduces the applicable civil penalty under the BIS settlement guidelines.[9]

[4] *Id*. at 4-6.

[5] *Id*. at 6-7.

[6] *Id*. at 2.

[7] U.S. Department of Justice, "Deputy Attorney General Lisa Monaco Delivers Remarks at American Bar Association National Institute on White Collar Crime," (March 2, 2023), *available at* https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-monaco-delivers-remarks-american-bar-association-national.

[8] https://www.bis.doc.gov/index.php/enforcement. In addition, information about voluntary self-disclosures for boycott violations can be found in Part 764.8 of the EAR.

[9] *See* Supplement No. 1 to Part 766 of the EAR.

Last June, the Office of Export Enforcement (OEE) implemented a dual-track system to handle VSDs.[10] VSDs involving minor or technical infractions are now resolved on a fast-track basis, with the issuance of a warning or no-action letter within 60 days of final submission. For those VSDs that indicate potentially more serious violations, OEE will do a deeper dive to determine whether enforcement action may be warranted, while at the same time adhering to the principle that companies deserve, and will get, significant credit for coming forward voluntarily. By fast-tracking the minor violations while assigning specific personnel to the potentially more serious ones, OEE is using its finite resources more effectively while also allowing companies that submit more minor VSDs to receive a quicker turnaround.

On April 18, 2023, the Assistant Secretary for Export Enforcement issued a memorandum regarding the BIS policy on voluntary self-disclosures and disclosures concerning others.[11] The memorandum clarifies the risk calculus on disclosures in two ways: first, a deliberate non-disclosure of a significant possible violation of the EAR will be considered an aggravating factor under BIS penalty guidelines. Second, if an entity becomes aware that another party is potentially violating the EAR and submits a tip to OEE, OEE will consider that a mitigating factor under the penalty guidelines if the information leads to an enforcement action and if the disclosing entity faces an enforcement action (even if unrelated) in the future.

Additionally, companies cannot sidestep the "should we voluntarily self-disclose or not" decision by self-blinding and choosing not to do an internal investigation in the first place. The existence, nature, and adequacy of a company's compliance program, including its success at self-identifying and rectifying compliance gaps, is itself considered a factor under the settlement guidelines.[12]

Together, the private sector and the U.S. Government can ensure that advanced American technologies do not reach those who would use such technologies to conduct activities of national security or foreign policy concern, including modernizing their military capabilities or committing human rights abuses.

DEPARTMENT OF THE TREASURY'S OFFICE OF FOREIGN ASSETS CONTROL'S VOLUNTARY SELF-DISCLOSURE POLICY

The Department of the Treasury's Office of Foreign Assets Control (OFAC) similarly encourages voluntary disclosures of apparent sanctions violations. As set forth in its Enforcement

[10] Memorandum from Matthew S. Axelrod, Assistant Secretary for Export Enforcement, to All Export Enforcement Employees, Re: Further Strengthening our Administrative Enforcement Program (June 30, 2022), *available at* https://www.bis.doc.gov/index.php/documents/enforcement/3062-administrative-enforcement-memo/file.

[11] Memorandum from Matthew S. Axelrod, Assistant Secretary for Export Enforcement, to All Export Enforcement Employees, Re: Clarifying Our Policy Regarding Voluntary Self-Disclosures and Disclosures Concerning Others (April 18, 2023), *available at* https://www.bis.doc.gov/index.php/documents/enforcement/3262-vsd-policy-memo-04-18-2023/file.

[12] *See* Section III.E to Supplement No. 1 to Part 766 of the EAR.

Guidelines,[13] OFAC considers VSDs to be a mitigating factor when determining appropriate enforcement action to take in response to a particular case. Additionally, in cases where a civil monetary penalty is warranted, a qualifying VSD can result in a 50 percent reduction in the base amount of a proposed civil penalty. In reviewing the underlying conduct in a VSD, OFAC considers the totality of the circumstances surrounding the apparent violation, including, among other factors, the existence, nature, and adequacy of the subject's compliance program at the time of the apparent violation and the corrective actions taken in response to an apparent violation.

Qualifying VSDs must occur prior to, or simultaneous with, the discovery by OFAC or another government agency of the apparent violation or a substantially similar apparent violation. Whether a notification of an apparent violation through a VSD to another agency will qualify as a VSD to OFAC is determined on a case-by-case basis.

Disclosures to OFAC will not qualify as VSDs under certain circumstances, including situations in which:

- a third party is required to and does notify OFAC of the apparent violation because the transaction was blocked or rejected by that third party (regardless of when OFAC receives such notice or whether the subject person was aware of the third party's disclosure);
- the disclosure includes false or misleading information;
- the disclosure is not self-initiated (including when the disclosure results from a suggestion or order of a federal or state agency or official; or, when the subject person is an entity, the disclosure is made by an individual in a subject person entity without the authorization of the entity's senior management. Responding to an administrative subpoena or other inquiry from, or filing a license application with, OFAC is not a VSD.); or
- the disclosure (when considered alongside supplemental information) is materially incomplete.[14]

OFAC requires VSDs to include—or to be followed within a reasonable period of time by—a sufficiently detailed report that provides a complete understanding of the circumstances of the apparent violation(s). Persons disclosing violations should be responsive to any follow-up inquiries by OFAC.

Conclusion

The benefits of VSDs are clear. In addition to making companies eligible for significant mitigation, disclosures provide an opportunity for companies to alert key national security

[13] *See* Appendix A to 31 CFR Part 501.

[14] *Id.* at I.I (Definitions - "Voluntary self-disclosure").

agencies to activities that may pose a threat to the national security and foreign policy objectives of the United States. Responsible companies who step forward help not only themselves, but also the interests of the U.S. Government and the American people, in advancing these important goals.

FINCEN'S ANTI-MONEY LAUNDERING AND SANCTIONS WHISTLEBLOWER PROGRAM

In addition to the benefits from disclosures about third parties offered by BIS described above, there can be monetary rewards for such reporting in certain circumstances. Specifically, the Financial Crimes Enforcement Network (FinCEN) maintains a whistleblower program designed to incentivize individuals in the United States and abroad to provide information to the government about violations of U.S. trade and economic sanctions, in addition to violations of the Bank Secrecy Act (BSA). Individuals who provide information to FinCEN or the Department of Justice may be eligible for awards totaling between 10 to 30 percent of the monetary sanctions collected in an enforcement action, if the information they provide ultimately leads to a successful enforcement action.

In certain circumstances, FinCEN may pay awards to whistleblowers whose information also led to the successful enforcement of a "related action," meaning that the agency could pay awards on enforcement actions taken under authorities such as the Export Control Reform Act.

Individuals may choose to disclose their identity when submitting information or they may remain anonymous. Individuals proceeding anonymously must be represented by legal counsel. Under 31 U.S.C. § 5323, there are certain confidentiality protections to individuals submitting information as well as certain protections from retaliation by employers.

FinCEN is currently accepting whistleblower tips. Individuals with questions about the whistleblower program, including questions about how best to submit information, should contact FinCEN through its website, www.fincen.gov/contact.