

August 2023

Follow @Paul_Hastings



DOJ OFAC BIS Joint Compliance Note and Enhanced Coordination Highlights Increased Enforcement Risk

By [Tom Best](#), [Nathaniel Edmonds](#), [Scott Flicker](#), [Lindsey Dieselman](#) & [Thomas Jordan](#)

On July 26, 2023, the U.S. Departments of Justice, Treasury, and Commerce issued a [joint compliance note](#) (“JCN”) regarding voluntary self-disclosure (“VSD”) policies that apply to potential violations of U.S. sanctions regulations, export control laws, and other national security laws. The JCN highlighted recent updates and new guidance for each department’s VSD policies and underscored the recent evolution of U.S. federal law enforcement agency efforts toward coordination and information-sharing among agencies and with other countries, resulting in heightened risk for companies operating internationally.

While the respective updates do not change the departments’ existing VSD policies, the JCN highlights the coordinated approach that U.S. enforcement agencies are emphasizing, creating an increased risk of enforcement of economic sanctions, export controls, and other national security-related rules and regulations. For all three enforcement authorities, the benefits and incentives for companies to voluntarily self-disclose potential criminal or civil violations of U.S. sanctions regulations, export control laws, or other national security laws generally rely upon whether 1) the disclosure was **prompt and timely**; 2) disclosures were **comprehensive** and contained all relevant information known at the time; 3) the company has **fully cooperated**; 4) there were **aggravating or mitigating factors** related to the conduct; and 5) the company **promptly remediated**. Companies that voluntarily self-disclose pursuant to the applicable VSD policies can benefit significantly from reduced civil penalties, more lenient forms of criminal resolutions, and lesser fines. While the VSD considerations are not new, the newly coordinated enforcement approach suggests that companies should carefully analyze their risks by conducting an integrated sanctions and export controls risk assessment, and ensure any investigation addresses the interests of all relevant authorities—the Departments of Justice, Commerce, and Treasury.

I. Updates to the Department of Justice’s National Security Division’s VSD Policy

The U.S. Department of Justice’s (“DOJ”) National Security Division (“NSD”) issued an [updated VSD policy](#) on March 1, 2023 concerning voluntary disclosures of potential criminal violations of U.S. sanctions regulations, export control, and national security laws. Pursuant to the updated policy, if a company reasonably promptly voluntarily self-discloses potential criminal violations, fully cooperates, and timely and appropriately remediates the violations, then NSD generally will not seek a guilty plea and there will be a presumption that the company will receive a non-prosecution agreement. Companies also will not be required to pay a fine if these circumstances are met; the updated guidance also

indicates, however, that qualifying companies will not be permitted to retain any unlawfully obtained gains relating to the underlying violations or underlying misconduct. Thus, companies will be subject to disgorgement or forfeiture requirements in any non-prosecution agreement.

This is similar to the DOJ Criminal Division's [Corporate Enforcement Policy](#) most recently [revised on January 17, 2023](#), and suggests an overall policy alignment between different DOJ divisions responsible for corporate criminal enforcement. The Criminal Division policy offers a presumption of a declination, as opposed to a non-prosecution agreement for NSD. However, the presumptions for a declination or a non-prosecution agreement do not apply when certain aggravating factors—such as egregious or pervasive criminal misconduct; upper management involvement; repeated violations; involvement of particularly sensitive technology or items, or end users of heightened concern; or significant profits stemming from the misconduct—are present. These limitations are consistent with the Corporate Enforcement Policy, with variations limited to factors unique to national security contexts, such as whether conduct involved a grave threat to national security, and are critical factors to consider when evaluating a company's strategy on disclosure.

The recent updates to the NSD VSD policy also mirror additional aspects of the Corporate Enforcement Policy, with many mirroring that document word-for-word. Specifically, as part of its updated VSD policy, NSD has clarified several of the requisite elements for obtaining credit. NSD's updated VSD policy clarified that "full cooperation" includes the timely preservation and collection of relevant documents, de-confliction of the company's internal investigative steps (including witness interviews), and timely identification of additional areas of investigation by NSD. The updated NSD VSD policy's definition of "full cooperation" now directly matches the Corporate Enforcement Policy. With respect to remediation, the NSD's updated VSD policy also now matches the Corporate Enforcement Policy, incorporating requirements that NSD must consider whether a subject company has implemented appropriate disciplinary measures for employees involved in or who had supervisory authority related to the criminal misconduct. The harmonization of the NSD VSD policy with the Corporate Enforcement Policy facilitates clearer and more consistent guidance for companies that often encounter compliance issues that span multiple DOJ divisions and policies.

In addition to updating these VSD guidelines, NSD has also recently hired a Chief Counsel for Corporate Enforcement and added 25 new prosecutors, further demonstrating DOJ's commitment to investigating and enforcing corporate compliance with national security laws.¹ Considering the FCPA Unit has only approximately 30 prosecutors focused on FCPA enforcement, these additional personnel resources within NSD add to the validity of Deputy Attorney General Lisa Monaco's statements that the DOJ will be devoting additional enforcement resources to national security issues, and that such issues are an ongoing enforcement priority.²

II. Updated VSD Guidance for the Department of Commerce's Bureau of Industry and Security

Also on July 26, in remarks to the Society for International Affairs, the Commerce Department Assistant Secretary for Export Enforcement Matthew Axelrod noted that an agreement had just been signed with OFAC "formalizing our close coordination and partnership. . . . we'll ensure that our enforcement teams are working even more closely together. . . . we'll be seeking to jointly resolve investigations of common subjects, including matters voluntarily disclosed to both agencies. As a result, you can expect to see more coordinated enforcement actions from us going forward."³ In May, Axelrod had remarked that the joint Disruptive Technology Strike Force which the Departments of Commerce and Treasury had formed in February 2023 was "starting to see results."⁴

The JCN does not introduce any changes to the Department of Commerce’s Bureau of Industry and Security’s (“BIS”) VSD policy. The JCN does highlight, however, administrative and resource allocation-related decisions internal to BIS intended to resolve minor infractions quickly, and focus on more important enforcement matters. The JCN explains that in addition to requiring VSDs to be timely, comprehensive, and involve full cooperation, in June of 2022 BIS implemented a new “dual-track” system for handling VSDs which stipulated that VSDs for minor or technical infractions would be resolved within 60 days, while more serious potential violations would receive a more in-depth review. The JCN also called attention to BIS’s [April 18, 2023 memorandum](#), which 1) noted that multiple minor or technical violations occurring close in time may be submitted in one VSD, and 2) clarified how BIS would apply its guidelines when a deliberate decision not to disclose is made.

In the April 2023 memorandum, BIS stated that it would consider a decision not to disclose as an aggravating factor for significant potential violations. This strategy differs from DOJ’s Corporate Enforcement Policy, for example, which does not specifically state that a failure to disclose is itself an aggravating factor, and instead states that a company which does not voluntarily disclose, “but later fully cooperated and timely and appropriately remediated . . . will receive, or the Criminal Division will recommend,” a reduction in penalties.⁵

The April memorandum also stipulated that—while it is not clear how the policy will work in practice—a third party that provides information regarding an apparent violation to BIS could receive mitigation credit for a future violation by that third party, even if the violation is not related to the conduct it reported to BIS. This policy also differs from DOJ and OFAC, which have not specifically stated that they will consider reporting another entity’s violations as a mitigating factor in the future.

The JCN reiterates BIS’s policy points from the April 2023 memorandum and also explains that BIS could regard as a negative factor a circumstance where a company that chose not to conduct an internal investigation into potential misconduct in order to avoid identifying evidence that could trigger a decision whether or not to disclose (i.e., seeking to remain “blind” to a potential violation), as such conduct could adversely affect BIS’s evaluation of the existence, nature, and adequacy of the company’s compliance program.

III. VSD Guidance from the Department of the Treasury’s Office of Foreign Assets Control

Similar to the NSD and BIS policies for VSDs, the Department of the Treasury’s Office of Foreign Assets Control (“OFAC”) has previously issued guidelines, see Appendix A to 31 C.F.R. Part 501, providing explicit incentives for companies to voluntarily self-disclose apparent violations of U.S. sanctions regulations in an environment where OFAC is “carving new paths in [its] technical work to target, monitor, and enforce sanctions.”⁶

The JCN also does not raise any new updates to OFAC’s enforcement guidelines. However, the JCN reiterates how OFAC considers VSDs and other mitigating (or aggravating) factors in assessing potential violations of U.S. sanctions regulations, including the impact of such factors upon the scope of potential applicable civil penalties. For example, in connection with the JCN, OFC Director Andrea Gacki has explained that companies taking advantage of OFAC’s VSD policy “can both help themselves and help us protect our financial system.”⁷ The JCN also highlights the importance of VSDs as a crucial mitigating factor under OFAC’s totality-of-the-circumstances assessment of apparent violations, where a qualifying VSD can result in a 50% reduction in the base amount of a proposed civil penalty. Finally, the JCN calls attention to OFAC’s requirement that to qualify, a VSD must occur prior to or simultaneously with OFAC’s

or another government agency's discovery of the apparent violation, and that OFAC considers on a case-by-case basis whether a VSD to another agency will qualify as a VSD to OFAC.

IV. The Role of the Department of the Treasury's Financial Crimes Enforcement Network

The JCN also highlights the expanded role of the Financial Crimes Enforcement Network's ("FinCEN") whistleblower program, which provides monetary rewards for whistleblower reports that lead to successful civil or criminal enforcement actions. While the FinCEN whistleblower program originally addressed only reported violations of the Bank Secrecy Act, Congress expanded the program after Russia's invasion of Ukraine to also provide whistleblower protections and monetary rewards concerning reports of potential violations of U.S. sanctions regulations and export control laws.

Under this expanded whistleblower program, potential whistleblowers can now report violations of U.S. sanctions regulations or export control laws to FinCEN, which would be referred onward to OFAC, BIS, and/or DOJ, as applicable, further demonstrating the coordinated approach among U.S. authorities. The JCN notes that in some cases "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."⁸ This creates an additional incentive for whistleblowers to report events that they believe to be violations of sanctions regulations or export control laws. FinCEN's role in sanctions and export control enforcement is likely to increase—notably, OFAC director Andrea Gacki was appointed to take over as director of FinCEN on July 13, 2023.⁹

V. Integrated Sanctions / Export Controls Risk Assessment

Given the rapid expansion of sanctions and export controls against Russia since its invasion of Ukraine in February 2022¹⁰—including increased U.S. coordination with its allies¹¹—and the increasing restrictions on exports of advanced technology to China,¹² companies are encountering unprecedented enforcement risks. Unfortunately, many companies' sanctions and export controls compliance programs were designed for a different era, when policies and procedures were focused on a more limited group of product types or a set of countries with complete bans on exports. Companies should seek to understand and address these new risks before small violations become systemic and before whistleblowers seek to monetize control failures.

To enhance their internal controls to meet this challenging new environment, companies should take the opportunity to conduct an integrated sanctions and export controls risk assessment, analyzing multiple regulatory regimes to ensure a coordinated approach rather than the more limited approach historically followed by many companies. An integrated sanctions and export controls risk assessment would include:

- Risk Identification, to include risks arising from the differing restrictions and interplay overlapping regulatory regimes, both among various U.S. agencies and between U.S. and other legal regimes, such as U.K. and EU restrictions.
- Analysis of Inherent Risk Ranking, factoring in a) the risks arising from doing business in a country with restrictions on some, but not all, exports, financial flows, and business relationships and b) the risk of diversion of exports from an authorized recipient or location to ones that are unauthorized.

- Identification and Rating of Mitigating Controls, including heightened monitoring based on risk identification and ranking, strengthened contractual terms, and restrictions on recipients' ability to transfer products, technology, or otherwise deal with sanctioned parties.
- Residual Risk Analysis, with a focus on auditing prior transactions and counterparties to ensure that potential violations are identified and reported in a timely manner.

Only by understanding the risks posed in the current regulatory enforcement environment can a company properly analyze how best to respond, and, ultimately, what the exposure will be if faced with a decision to voluntarily disclose potential misconduct.

Conclusion

Overall, the JCN highlights the evolving U.S. position in coordinating investigative efforts and sharing information among enforcement authorities. Notably, in May of this year, BIS's Matthew Axelrod remarked that a group of indictments for illegal shipments to China and Russia were "just the beginning," and that such actions could be "expect[ed] to continue" to be seen from the Disruptive Technology Strike Force.¹³ Enhanced cooperation among U.S. agencies, as part of increasing multilateral cooperation among the U.S., U.K., EU, and others, is likely to develop and strengthen going forward.

While the JCN calls attention to the fact that each agency has its own policies and factors it considers when determining what mitigation a company should receive, it also indicates that common factors are completeness, cooperation, and the seriousness of the underlying conduct. In addition, both DOJ and BIS consider the timeliness of the VSD as an important factor; OFAC does not have a specific requirement for prompt disclosure but to qualify, a VSD must be made before OFAC or another agency discovers the conduct at issue, and OFAC will not automatically give credit for a VSD made to another agency.

Importantly, the inter-agency cooperation highlighted by the JCN indicates that deliberations over a potential disclosure decision during a company's internal investigation should take into account that any information disclosed is very likely to be shared among all agencies. Because each agency is likely to focus on different aspects of the underlying conduct, a company may face inquiries regarding the facts of the initial VSD that, in effect, uncover other potential violations. Consequently, a company undertaking an investigation into export controls or sanctions violations must look at it holistically and not look narrowly at one regulatory regime.

The U.S. enforcement authorities are signaling that an enforcement change is coming. Companies should heed their call and evaluate the strength of their export controls programs promptly. If issues are discovered, which is almost inevitable in this rapidly changing environment, then companies must face the difficult decision of whether to disclose—but they should only make that decision after thoroughly investigating how the facts implicate all the enforcement regimes that may be interested in the conduct.

◇ ◇ ◇

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings Washington, D.C. lawyers:

Tom Best
1.202.551.1821
tombest@paulhastings.com

Scott M. Flicker
1.202.551.1726
scottflicker@paulhastings.com

Thomas Jordan
1.202.551.1926
thomasjordan@paulhastings.com

Nathaniel B. Edmonds
1.202.551.1774
nathanieledmonds@paulhastings.com

Lindsey Ware Dieselman
1.202.551.1921
lindseydieselman@paulhastings.com

-
- ¹ 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>.
 - ² Indeed, Ms. Monaco has been quoted as stating that "sanctions are the new FCPA." U.S. Department of Justice, "Deputy Attorney General Lisa O. Monaco Delivers Keynote Remarks at 2022 GIT Live: Women in Investigations," (June 16, 2022), available at <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-keynote-remarks-2022-gir-live-women>.
 - ³ BIS, "Remarks as Prepared for Delivery by Assistant Secretary for Export Enforcement Matthew S. Axelrod to the Society for International Affairs Summer Back to Basics Conference" (July 26, 2023), available at <https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/3304-axelrod-sia-keynote-final/file>.
 - ⁴ BIS, "Assistant Secretary for Export Enforcement Matthew S. Axelrod Delivers Remarks on the Disruptive Technology Strike Force," (May 16, 2023), available at <https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3271-2022-05-16-as-axelrod-disruptive-tech-strike-force-announcement-final-1/file>.
 - ⁵ U.S. Department of Justice, 9-47.120 – *Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy*, (Jan. 2023), § 3, available at <https://www.justice.gov/criminal-fraud/file/1562831/download>.
 - ⁶ U.S. Dep't of the Treasury, "Remarks by Secretary of the Treasury Janet L. Yellen on Way Forward for the Global Economy" (Apr. 13, 2022), available at <https://home.treasury.gov/news/press-releases/jy0714>.
 - ⁷ U.S. Dep't of Justice, "Departments of Justice, Commerce and Treasury Issue Joint Compliance Note on Voluntary Self-Disclosure of Potential Violations" (July 26, 2023), available at <https://www.justice.gov/opa/pr/departments-justice-commerce-and-treasury-issue-joint-compliance-note-voluntary-self>.
 - ⁸ The FinCEN whistleblower program is relatively new, having been set in place in 2021; in remarks made in March 2022, Himamauli Das, then acting director of FinCEN, stated that the program was in its early stages and that "To be eligible for an award, the whistleblower's information must lead to a successful enforcement action by FinCEN or DOJ." FinCEN, "Prepared Remarks of FinCEN Acting Director Himamauli Das During NYU Law's Program on Corporate Compliance and Enforcement," (Mar. 25, 2022) available at <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-director-himamauli-das-during-nyu-laws-program>.
 - ⁹ Dylan Tokar, "Treasury's Sanctions Chief Is Appointed Director of Financial Crimes Bureau," WALL STREET JOURNAL (July 13, 2023), available at <https://www.wsj.com/articles/treasurys-sanctions-chief-is-appointed-director-of-financial-crimes-bureau-9c75e6dc>.
 - ¹⁰ For example, since the invasion, OFAC has designated over 2,500 Russia-related entities as SDNs and has sanctioned more than 75% of the entities in operation in Russia's banking sector; FinCEN has issued four alerts, an advisory, and an analysis of trends and red flags associated with Russian illicit finance and corruption; the G7 and EU have adopted price caps on sales of crude oil originating in Russia (see, e.g., Dep't of the Treasury, "FACT SHEET: Disrupting and Degrading—One Year of U.S. Sanctions on Russia and Its Enablers," (Feb. 24, 2023) available at <https://home.treasury.gov/news/press-releases/jy1298#:~:text=Fast%20Stats,115%20vessels%2C%20and%2019%20aircraft.>); and BIS has implemented increased export controls targeting the defense, aerospace and marine, and oil refining sectors (see, e.g., "Departments of Justice, Commerce and Treasury Issue Joint Compliance Note on Russia-Related Sanctions Evasion and Export Controls," (Mar. 2, 2023) available at <https://www.justice.gov/opa/pr/departments-justice-commerce-and-treasury-issue-joint-compliance-note-russia-related#:~:text=Since%20Feb.,its%20illegal%20war%20in%20Ukraine.>), among other things.

Stay Current is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2023 Paul Hastings LLP.

other measures: Supplements No. 5 and 6 to 15 C.F.R. § 746 restrict the export to Russia or Belarus of, respectively, luxury goods that may facilitate money laundering and items useful to Russian chemical and biological weapons production capabilities).

- ¹¹ In addition to taking action to designate the same parties on their sanctions lists, the U.S., EU, and other allies are coordinating on additional measures, such as removing some Russian banks from the international SWIFT payments system. RFE/RL, “EU Cuts Seven Russian Banks from SWIFT, Bans RT and Sputnik,” (Mar. 2, 2022) available at <https://www.rferl.org/a/eu-swift-russian-banks/31732511.html>. See also Dep’t of the Treasury, “Targeting Key Sectors, Evasion Efforts, and Military Supplies, Treasury Expands and Intensifies Sanctions Against Russia,” (Feb. 24, 2023) available at <https://home.treasury.gov/news/press-releases/jv1296> (noting sanctions coordination between U.S. agencies “in coordination with allies and G7 partners[.]”) and Dep’t of the Treasury, “U.S. and EU Sanctions Teams Enhance Bilateral Partnership,” (May 16, 2023) available at <https://home.treasury.gov/news/press-releases/jv1485> (describing an April 2023 multilateral meeting in Brussels between OFAC, the European External Action Service, and the European Commission Directorate-General for Financial Stability, Financial Services and Capital Markets Union to strengthen working relationships).
- ¹² Restrictions on exports to China of advanced chips and semiconductors were put in place last year, BIS, “Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People’s Republic of China,” (Oct. 7, 2022) available at <https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file> (noting two new export control rules restricting China’s “ability to obtain advanced computing chips, develop and maintain supercomputers, and manufacture advanced semiconductors.”), and recent reports indicate that broader restrictions are being developed, see, e.g., Evelyn Cheng and Clement Tan, “Senate passes toned-down bill to increase oversight of investments in Chinese technology,” (July 26, 2023) available at <https://www.cnbc.com/2023/07/26/senate-passes-bill-to-increase-oversight-of-investments-in-chinese-technology.html> (noting that the law, if passed, “would require U.S. firms to notify the Treasury when investing in advanced Chinese technology on national security concerns.”) and Andrew Duehren, U.S. Prepares New Rules on Investment in China,” WALL STREET JOURNAL (Mar. 3, 2023) available at <https://www.wsj.com/articles/u-s-prepares-new-rules-on-investment-in-technology-abroad-a451e035> (noting that the Treasury and Commerce departments “were considering a new regulatory system to address U.S. investment in advanced technologies abroad that could pose national security risks” and that could “prohibit some investments while also potentially collecting information” about others and could “cover private-equity and venture-capital investments in advanced semiconductors, quantum computing and some forms of artificial intelligence.”).
- ¹³ Ian Cohen, “Recent Export Control Enforcement Actions ‘Just the Beginning,’ BIS Official Says” (18 May 2023), Export Compliance Daily, available at <https://exportcompliancedaily.com/news/2023/05/18/recent-export-control-enforcement-actions-just-the-beginning-bis-official-says-2305170033>.