



TORRES TRADE LAW

INTERNATIONAL TRADE & NATIONAL SECURITY



Voluntary Self-Disclosure Handbook

September 9, 2025 | Torres Trade Law, PLLC

Torres Trade Law, PLLC is an international trade and national security law firm that assists clients with the import and export of goods, technology, and services. The firm has extensive experience with the various regimes and agencies governing trade such as the Directorate of Defense Trade Controls, the Bureau of Industry and Security, the Office of Foreign Assets Control, the U.S. Customs and Border Protection and others. Our group provides clients with full support for all trade law issues, including U.S. export control and sanctions laws, industrial security, the Foreign Corrupt Practices Act, anti-boycott laws, and customs law.

This Voluntary Self-Disclosure Handbook has been prepared as an industry reference only, and is not official direction or instruction, nor does it constitute legal advice. It is not intended to be used in place of any U.S. Government statute, regulation, authorization, or guidance. This Voluntary Self-Disclosure Handbook is intended to provide a reference as of the date of publication and is not meant to be a comprehensive review of the pros and cons of filing disclosures. Please ensure that you consider any updates to U.S. Government statutes, regulations, or guidance that may have occurred since publication when you use this Torres Trade Law Voluntary Self-Disclosure Handbook.

TABLE OF CONTENTS

I. Introduction

- A. What are VSDs?
- B. Why file a VSD?
- C. What are the risks of a VSD?

II. Key Steps Prior to Filing a VSD

- A. Stop Any Potential Ongoing Violations
- B. Start Further Investigation Promptly
- C. Consult Counsel to Establish Legal Privilege Regarding Any Investigation
- D. Issue Legal Holds
- E. *Upjohn* Rights

III. Understand Which Government Regulators May be Involved in a VSD

IV. VSD Processes and Considerations for Key U.S. Regulators

- A. U.S. Department of Commerce, BIS
 - 1. Disclosure of Minor or Technical Violations
 - 2. Disclosure of Significant Violations
 - 3. Extensions of Time to Submit Final Narrative Account, 15 C.F.R. § 764.5(c)(2)(iv)
 - 4. Final Narrative Account, 15 C.F.R. § 764.5(c)(3)
 - 5. VSD Submission
 - 6. Potential Action by OEE, 15 C.F.R. § 764.5(d)
- B. U.S. Department of State, DDTC
 - 1. Initial Notification, 22 C.F.R. § 127.12(c)(1)
 - 2. Full Disclosure, 22 C.F.R. § 127.12(c)(1), (2)
 - 3. VD Submission
 - 4. Potential Action by DDTC
- C. U.S. Department of Commerce, Census
 - 1. Voluntary Self-Disclosures, 15 C.F.R. § 30.74
 - 2. Initial Notification, 15 C.F.R. § 30.74(c)(2)
 - 3. Narrative Account, 15 C.F.R. § 30.74(c)(3)
 - 4. VSD Submission
 - 5. Potential Action by Census 15 C.F.R. § 30.74(d)
- D. U.S. Department of the Treasury, OFAC
 - 1. Voluntary Self-Disclosures, 31 C.F.R. Appendix A to Part 501, (I)
 - 2. VSD Submission
 - 3. Potential Action by OFAC
- E. Department of Justice, Criminal Division, Corporate Enforcement and Voluntary Self-Disclosure Policy
 - 1. Voluntary Self-Disclosure
 - 2. VSD Submission
 - 3. Potential Action by DOJ
 - 4. 2025 Updates to Enforcement Focus
- F. Department of Justice, National Security Division (“NSD”), Enforcement Policy for Business Organizations
 - 1. Voluntary Self-Disclosure
 - 2. VSD Submission
 - 3. Potential Action by DOJ

- G. Department of Justice, Commercial Litigation Branch, Guidelines for Taking Disclosure, Cooperation, and Remediation into Account in False Claims Act Matters
 - 1. Voluntary Self-Disclosure
 - 2. VSD Submission
 - 3. Potential Action by DOJ
- H. Department of Justice, U.S. Attorneys' Offices ("USAO"), Voluntary Self-Disclosure Policy
 - 1. Voluntary Self-Disclosure
 - 2. VSD Submission
 - 3. Potential Action by DOJ
- I. Department of Justice, Mergers & Acquisitions Safe Harbor Policy
- J. Department of Homeland Security, U.S. Customs and Border Protection
 - 1. Prior Disclosure ("PD"), 19 U.S.C. § 1592(c)(4) / 19 C.F.R. § 162.74
 - 2. PD Submission
 - 3. Potential Action by CBP

I. INTRODUCTION

A. What are VSDs?

A voluntary self-disclosure (“VSD”) (also known as voluntary disclosures or prior disclosures depending on the governing agency) is a narrative account with supporting documentation that describes violations or suspected violations of import, export, economic sanctions, or anti-corruption regulations, and ideally, describes a party’s efforts to mitigate the harm caused by such violations or efforts to remediate the causes of such violations. Most government agencies permit companies to file an Initial Notification of the VSD before submitting a full or final VSD. In general, the Initial Notification serves as a notice to the regulatory and enforcement agencies of the general nature and extent of the potential violations.

B. Why file a VSD?

Filing a VSD offers several benefits with respect to mitigating potential consequences associated with violations of U.S. trade laws. A VSD can:

- Reduce the likelihood and severity of an enforcement action by the relevant agencies, including the likelihood of prosecution when submitted to the U.S. Department of Justice (“DOJ”).
- Act as a mitigating factor when determining the amount and severity of penalties for violations.
- Help establish a positive relationship with the regulatory agencies.
- Reduce the likelihood of future violations.
- Help to avoid directed disclosures (disclosures required by a regulator, which limit ability to mitigate penalties for any violations).
- Reduce reputational harm.

C. What are the risks of a VSD?

Filing a VSD does entail some risk to the filer. Consult with qualified legal counsel prior to deciding to file a VSD to effectively assess these risks, which can include, but are not limited to:

- A VSD is an admission of improper conduct.
- A VSD creates knowledge of violations, which could create liability if “knowing” violations occur after disclosure.
- A VSD can lead to loss of confidentiality and waiver of privilege.
- Regulatory authorities may require waiver of certain defenses or extension (tolling) of statute of limitations on violations.
- Additional questions may follow, as well as increased regulatory scrutiny.
- Violations may involve other laws (beyond those related to international trade compliance), and criminal violations may be referred to the DOJ for prosecution.

II. KEY STEPS PRIOR TO FILING A VSD

A. Stop Any Potential Ongoing Violations

To the extent that specific potential violations have been identified (for example, items exported without a required export license), it is critical that steps are taken to stop similar additional violations. This may require institution of “stop-ship” orders, changes to physical or electronic access to technical data/technology, application to regulators for licenses or

agreements, or other remedial measures designed to stop ongoing violations and prevent, in the near term, future violations.

B. Start Further Investigation Promptly

As described below, it is also critical that upon filing an initial disclosure, further investigation of the nature, scope, cause, and impact of the potential or apparent violations is undertaken promptly and thoroughly documented. A thorough investigation plan should be prepared by the investigator and key witnesses, or potential interviewees identified.

C. Consult Counsel to Establish Legal Privilege Regarding Any Investigation

It is strongly recommended that the investigation of potential or apparent violations as part of a disclosure be conducted by, or at the direction of, an attorney, in order to preserve attorney-client privilege regarding advice and materials produced as a result of the investigation.

D. Issue Legal Holds

A legal hold (or litigation hold) must occur to preserve data potentially relevant to anticipated, pending, or active litigation, investigations, or other legal disputes. Issuing a legal hold is an essential early step in the discovery or investigation process, and crucial to showing defensible and good faith efforts to preserve evidence. The goal of preserving information is to ensure that the information's evidentiary integrity is maintained for potential use in the case.

E. *Upjohn* Rights

In an internal investigation an attorney acts on behalf of the corporation, which may have differing interests from those of the directors, officers, and employees through whom the corporation functions. One of the most important steps in reducing risk of a conflict is the *Upjohn* warning, which involves corporate counsel advising individual employees that counsel represents only the corporation and not the individual. Providing the *Upjohn* warning can avoid hazards for the corporation, the individuals, and counsel.

III. UNDERSTAND WHICH GOVERNMENT REGULATORS MAY BE INVOLVED IN A VSD

Various U.S. government agencies have different regulations, policies, and official guidance regarding the ability of parties to file VSDs, how such VSDs are assessed, and the impact such VSDs may have on enforcement actions.

For purposes of this handbook, we will focus on the U.S. Department of Justice ("DOJ"); the U.S. Department of Commerce, Bureau of Industry and Security ("BIS"); the U.S. Census Bureau ("Census"); the U.S. Department of State, Directorate of Defense Trade Controls ("DDTC"); the U.S. Department of the Treasury, Office of Foreign Assets Control ("OFAC"); and the U.S. Department of Homeland Security Customs and Border Protection ("CBP").

Keep in mind that other U.S. government agencies (and foreign agencies) involved in regulating other aspects of international trade may also have jurisdiction over the activities being disclosed – for example, the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") or the Food and Drug Administration ("FDA") – and the risks of

disclosure should also be assessed in this light as well.

It is common to file multiple disclosures amongst various agencies simultaneously to ensure that one agency does not share evidence of a potential or apparent violation with another agency before the disclosing party does (in which case a party may lose “credit” for the disclosure being “voluntary”).

The DOJ also has voluntary disclosure programs permitting submission of voluntary self-disclosures directly to a relevant DOJ component for potential violations of import, export control, and sanctions laws. The DOJ has indicated that such disclosures may “significantly” reduce criminal penalties, including “a non-prosecution agreement (“NPA”) or declinations to prosecute, a reduced period of supervised compliance, a reduced fine and forfeiture, and no requirement for a monitor.” As described below, companies typically submit initial disclosures to the regulatory agencies followed up by final disclosures at a later date, and the agencies have the discretion to refer criminal matters to DOJ during this period. In this case, companies may have to consider early in their investigation whether the circumstances demonstrate a potential benefit to filing a VSD with DOJ concurrently with self-disclosures with the other regulatory agencies.

IV. VSD PROCESSES AND CONSIDERATIONS FOR KEY U.S. REGULATORS

As described below, each regulatory or enforcement agency has different procedures and requirements regarding how disclosures must be filed, what information must be provided, and the process for evaluating regulatory or enforcement actions based on such disclosures. As noted above, evaluating the potential risks and benefits of filing a disclosure should be determined with respect to each regulatory or enforcement agency based on the specific facts of the case and with consultation of upper management and legal counsel.

A. U.S. Department of Commerce, Bureau of Industry and Security

The Department of Commerce BIS is primarily engaged in regulating the export, reexport, and transfer of commercial items and technology having dual commercial and military applications controlled under the Export Administration Regulations (“EAR”).

1. Disclosure of Minor or Technical Violations, 15 C.F.R. § 764.5(c)

Minor or Technical violations are those that do not involve aggravating factors as defined in 15 C.F.R. Part 766, supplement no. 1, section III(A). An abbreviated narrative report may be submitted to BIS that includes the following information:

- Name of the person making the disclosure, designated contact person, the contact person’s current business street address, email, and telephone number;
- A description of the general nature and extent of the violations; and
- A description of additional minor or technical violations (if applicable) if such violations occurred within the preceding quarter.

The Director of the BIS Office of Export Enforcement (“OEE”) may at their discretion request the disclosing party to submit a full narrative report pursuant to 15 C.F.R. § 764.5(d)(3) within 180 days of the date of the OEE Director’s request.

2. Disclosure of Significant Violations, 15 C.F.R. § 764.5(d)

Violations that do not involve technical or minor infractions as defined in 15 C.F.R. Part 766, supplement no. 1, section III(A) may be voluntarily disclosed to BIS via an initial notification and a subsequent final narrative submission.

The Initial Notification should be made to the BIS OEE in writing as soon as possible after violations are discovered. This notification should include:

- Name of the person making the disclosure and a brief description of the potential violation;
- A contact person with business address, email, and phone number; and
- A description of the general nature and extent of the potential violations.

The Initial Notification is considered valid as of the date that the notification is received by OEE. A final narrative account is due 180 days from OEE's receipt of the Initial Notification.

3. Extensions of Time to Submit Final Narrative Account, 15 C.F.R. § 764.5(d)(2)(iv)

OEE can grant an extension at its discretion if such an extension serves the government's interests or if the requesting company has shown reasonable need. There may also be conditions placed on the granting of an extension. In order to be considered, a request must show:

- A review was started promptly after discovery of violations.
- The review and preparation of narrative had been conducted expeditiously, completely, and accurately.
- Interim compliance procedures have been considered/identified to prevent further violations.
- A reasonable need for the extension.
- A timeline for completion and submission of the narrative; a designated contact person and contact person's business address, email address, and telephone number; and additional information the person making the request reasonably believes is pertinent.

4. Final Narrative Account, 15 C.F.R. § 764.5(d)(3)

After the Initial Notification, the disclosing party should conduct a thorough review for all export-related transactions involving the suspected violations. OEE recommends that the review cover a period of five years prior to the date of the Initial Notification (the statute of limitations for export violations is five years). After review, a narrative account must be submitted to OEE describing the nature of the review conducted, suspected violations, and measures taken to minimize violations and prevent future violations. The narrative must include:

- The type of violation—for example, describing exports of hardware that occurred without a required export license and deemed exports of technology to foreign person employees.
- Explanation of when and how violations occurred—for example, identifying the period of time during which unauthorized exports occurred and the causes of the violations, such as misclassification of items.
- Complete identities and addresses of all individuals and organizations involved in activities giving rise to violations—this may include subsidiaries, affiliates, and third parties.

- License numbers—licenses associated with any unauthorized exports that are being disclosed.
- Description, quantity, value (U.S. dollars), and Export Control Classification Number or other classification of the items involved.
- Description of mitigating circumstances—these may include such factors as:
 - The size and sophistication of the party having committed the violations.
 - Existence of a compliance program designed to identify potential violations.
 - Efforts to remediate issues that lead to violations.
 - Likelihood that any unauthorized exports would have been licensed.
 - Cooperation with the agency.
 - Regulatory/criminal history of the party.

Additional Information for Final Narrative

- Supporting Documentation, § 764.5(d)(4)
 - Along with the narrative, copies of licensing documents, shipping documents, and other documents such as invoices, purchase orders, or communications.
 - Any other relevant documents should also be included.
- Certification, § 764.5(d)(5)
 - Must certify that all of the representations made in connection with the VSD are true and correct to the best of disclosing person's knowledge and belief.
- Oral Presentations § 764.5(d)(6)
 - An oral presentation to OEE may be requested but is not necessary.

5. VSD Submission

All VSD submissions, including those concerning minor or technical violations, should be submitted electronically via email to BIS_VSD_INTAKE@bis.doc.gov. VSDs may also be submitted in hard copy to the following address:

Director, Office of Export Enforcement
 1401 Constitution Ave., Room H4514
 Washington, D.C. 20230.

6. Potential Action by OEE, 15C.F.R. § 764.5(e)

OEE will issue a formal acknowledgement of receipt of the disclosure. OEE may then take any of the following actions:

- For disclosures of minor or technical violations, OEE will generally resolve the matter within 60 days of the VSD submission date and either take no action or issue a warning letter.
- OEE, at its discretion, may take no action or issue a warning letter in cases involving more significant violations.
- Issue a proposed charging letter and attempt to settle.
- Issue charging letter (if settlement not reached).
- Administrative actions, including denial of, or restriction on, a party's export/import privileges.
- Refer to DOJ for criminal prosecution (rare in VSD cases).

B. U.S. Department of State, Directorate of Defense Trade Controls

DDTC is primarily engaged in the regulation of the export/import of defense articles, technical data, and defense services controlled under the International Traffic in Arms Regulations (“ITAR”).

1. Initial Notification, 22 C.F.R. § 127.12(c)(1)

An initial notification of a Voluntary Disclosure (DDTC refers to a disclosure as a “VD”) should be made to DDTC in writing immediately after violations are discovered. A notification will be considered filed upon receipt by DDTC. A new disclosure will be assigned a DDTC case number typically within 5-10 days and DDTC will notify the disclosing party of such action via email.

2. Full Disclosure, 22 C.F.R. § 127.12(c)(1), (2)

A final VD must be submitted within 60 days of the initial notification; extensions may be granted in some circumstances. If not timely filed or no extension is requested, then DDTC may choose not to consider the VD as a mitigating factor. The VD should be in writing and contain the following elements (which will be similar in scope to those described for disclosures to BIS):

- Precise nature and extent of the violations. Circumstances of the violations.
- Identities and addresses of all persons involved.
- Department of State license numbers, exemptions citations, or description of any other authorization (if applicable).
- U.S. Munitions List category and subcategory, product description, quantity, and characteristics of the hardware, technical data, or defense service involved.
- Description of corrective actions already taken and how actions are designed to deter future violations. Name and address of person making disclosure and point of contact.
- Mitigating factors, including but not limited to:
 - No prior violations.
 - Whether person had knowledge of laws and regulations.
 - Compliance/remedial measures.
 - Review of export transactions.
 - Whether violations are systemic or intentional.

Additional Information for Final VDs:

- Documentation, § 127.12(d)
 - The VD should be accompanied by substantiating documents, including:
 - Licensing documents, exemption citation, or other authorization description.
 - Shipping documents; and any other relevant documents.
- Certification, § 127.12(e)
 - Certification stating that all representations made are true and correct to the best of that person’s knowledge and belief and should be executed by an empowered official or senior officer.
- Oral Presentations, § 127.12(f)
 - Oral presentations are not required but can be requested in writing, if desired.

3. VD Submission

VDs can be electronically submitted to the Office of Defense Trade Controls Compliance, Directorate of Defense Trade Controls via email to DTCC-CaseStatus@state.gov. VDs may also be submitted by delivery to one of the relevant addresses listed below:

By Courier:

U.S. Department of State
PM/DDTC, SA-1, 12th Floor
2401 E Street, NW
Washington, D.C. 20037

By mail:

PM/DDTC, SA-1, 12th Floor
Directorate of Defense Trade Controls
Bureau of Political-Military Affairs,
U.S. Department of State
Washington, D.C. 20522

4. Potential Action by DDTC

DDTC may take a range of actions in response to a VD, including:

- Close-out letter;
- Follow up questions or document requests;
- Recommended compliance actions (e.g., appointment of independent auditor);
- Issue charging letter;
- Civil consent agreement (typically involving a monetary penalty and compliance monitor); and
- Referral to DOJ for criminal prosecution (rare in VD cases).

C. U.S. Department of Commerce, Census Bureau

Census regulates filings related to imports to, and exports from, the United States covered under the Foreign Trade Regulations (“FTR”).

1. Voluntary Self-Disclosures, 15 C.F.R. § 30.74

- VSDs are only considered voluntary if submitted before Census or another agency learns of the information.
- VSDs are mitigating factors but can be outweighed by aggravating factors.
- Senior management must have full knowledge and authorization of the disclosure.
- Conduct a thorough review of all export transactions for past five years and notify Census of the violations.

2. Initial Notification 15 C.F.R. § 30.74(c)(2)

- The Initial Notification must be in writing and sent to the proper address.
- Include the name of the person making the disclosure and a brief description of the potential violations (general nature, circumstances, and extent of violations).
- If the person making the disclosure subsequently completes the narrative account, the disclosure will be deemed to have been made on date of the Initial Notification.

3. Narrative Account 15 C.F.R. § 30.74(c)(3)

- The review period should cover a period of five years prior to date of the Initial Notification.
- The narrative must sufficiently describe nature and gravity of suspected violations; it must also include the nature of review conducted and measures taken to minimize the likelihood of future violations.
- Additionally, the narrative should include:
 - Type(s) of violations involved;
 - Description of data not reported or reported incorrectly;
 - How and when violations occurred;
 - Identities and addresses of all individuals and organizations involved in activities giving rise to the violations;
 - Mitigating circumstances;
 - Corrective measures taken;
 - Internal Transaction Numbers (“ITNs”) of missed or corrected shipments; and
 - Electronic Export Information: In a Census VSD you will be required to correct EEI filings with errors. Report all data required by the Foreign Trade Regulations that was not reported, or corrections for all data reported incorrectly.
- Note that as of March 3, 2025, the Census TRB has implemented the use of a “VSD Form.” The VSD Form outlines the specific information required to be included in a final narrative account pursuant to 15 C.F.R. § 30.74(c)(3) and contains fillable blocks for a disclosing party to input relevant information. A disclosing party’s final narrative account should be submitted on the VSD Form available at the following web address:

<https://www.census.gov/foreign-trade/regulations/vsd.html>

4. VSD Submission 15 C.F.R. § 30.74(c)(5)

VSDs should be submitted electronically to the Census Trade Regulations Branch (“TRB”). The final VSD should be submitted on the Census VSD Form and emailed in a password-protected file to emd.askregs@census.gov. Initial disclosures may be submitted electronically on company letterhead and addressed to:

Chief, Economic Management Division
U.S. Census Bureau
4600 Silver Hill Road,
Suitland, MD 20746

5. Potential Action by Census 15 C.F.R. § 30.74(d)

Census does not have its own enforcement branch, so it relies on CBP and OEE to enforce penalties for FTR violations. After a final VSD is submitted, Census may take the following actions:

- Upon receipt of the narrative, Census may notify CBP, Immigration and Customs Enforcement (“ICE”), and OEE of the VSD and may acknowledge the disclosure by letter.
- Provide a point of contact to the person who disclosed the potential violations.
- Take actions it deems appropriate, which may include:
 - Inform the organization or individual that submitted the VSD of the action to be taken.
 - Issue a warning letter or letter setting forth corrective measures required.

- Refer the matter to OEE.

D. U.S. Department of the Treasury, Office of Foreign Assets Control

OFAC is primarily responsible for regulating and enforcing U.S. economic sanctions laws.

1. Voluntary Self-Disclosures, 31 C.F.R. Appendix A to Part 501, (I)

- A VSD must be self-initiated (not directed or requested by OFAC or as a result of a third-party report of a blocked or rejected transaction) and include, either initially or within a reasonable time, a report of sufficient detail to afford complete understanding of the circumstances of the apparent violations of specified statutes, Executive Orders, or regulations.
- A VSD will not be considered valid if it contains false or misleading information, is materially incomplete, or is made without knowledge or authorization of senior management.
- A VSD should address the nature, scope, and cause of apparent violations as well as potentially mitigating factors, including:
 - Willfulness or recklessness – whether the conduct was intentional or demonstrates intentional disregard.
 - Concealment – whether there were efforts to conceal the violations.
 - Pattern of conduct – whether there were multiple related violations.
 - Awareness – whether there was awareness of the violations.
 - Management involvement in conduct that resulted in the violations.
 - Whether the violations resulted in harm to sanctions program objectives.
 - An existing sanctions compliance program in place.
 - Appropriate remedial response to prevent additional violations.
 - History of violations.
 - Cooperation with OFAC in disclosure and any subsequent investigation.

2. VSD Submission

OFAC requests that all VSDs be submitted electronically by email to OFACDisclosures@treasury.gov.

3. Potential Action by OFAC

- No action.
- Request for additional information.
- Cautionary letter warning of potential for misconduct.
- Finding of violation without penalty.
- Civil monetary penalty (typically the result of a settlement agreement)—OFAC may determine whether a civil penalty is warranted by first issuing a pre-penalty notice, and providing an opportunity to respond, prior to issuance of a penalty notice.
 - Cases deemed “egregious” may be given the largest fines (half of applicable statutory maximum penalty if VSD submitted; without a VSD, the maximum penalty may be applied).

- Referral to DOJ for criminal prosecution.
- Administrative actions such as license denial, cease and desist order, etc.

E. Department of Justice, Criminal Division, Corporate Enforcement and Voluntary Self-Disclosure Policy

The DOJ's Criminal Division handles corporate criminal matters, including, but not limited to, cases involving violations of the Foreign Corrupt Practices Act ("FCPA").

1. Voluntary Self-Disclosure

- To receive credit under the Criminal Division's VSD policy, a disclosing party must submit a VSD to the Criminal Division, fully cooperate with the Criminal Division's investigation, and implement timely and appropriate remedial measures.
- A disclosing party may receive credit under this policy if it submits a VSD in "good faith" to another DOJ office or component and the resolution includes the Criminal Division.
- A VSD must be made "within a reasonably prompt time" after the company becomes aware of the misconduct and "prior to an imminent threat of disclosure or government investigation."
- A VSD must contain all relevant facts known to the company at the time of the disclosure, including the identity of individuals substantially involved in, or responsible for, the misconduct.
- Full cooperation requires timely disclosure (within the VSD or via subsequent updates to the Criminal Division) of all non-privileged facts relevant to the misconduct at issue, including:
 - All relevant facts gathered during a company's independent investigation;
 - Attribution of facts to specific sources where such attribution does not violate the attorney-client privilege, rather than a general narrative of the facts;
 - Timely updates on a company's internal investigation, including but not limited to rolling disclosures of information;
 - All facts related to involvement in the subject criminal activity by the company's officers, employees, or agents.
- Production of documents, witnesses for interviews, including overseas documents and employees and agents may be required.
- The VSD should include a description and timeline of the steps the company is taking to remediate the disclosed conduct, including a root cause analysis, outline of the implementation or enhancement of a compliance and ethics program, and an overview of disciplinary actions that were taken.
- Aggravating factors include involvement of senior executives in the misconduct, significant profit from the misconduct, pervasiveness of the misconduct within the company, and whether the company is a repeat offender.

2. VSD Submission

Individuals and companies wishing to disclose information about potential FCPA violations are encouraged to contact the FCPA unit at the telephone number or email address below.

DOJ Contact Information:

Fraud Section, Criminal Division
U.S. Department of Justice
ATTN: Chief, FCPA Unit
950 Constitution Avenue, N.W.
Washington, D.C. 20530
Email: fcpa.fraud@usdoj.gov

3. Potential Action by DOJ

- The Criminal Division will decline prosecution where a company (1) submits a VSD to the Criminal Division, (2) fully cooperates with the DOJ investigation, (3) implements timely and appropriate remedial measures, and (4) no aggravating circumstances are present.
- In cases where aggravating circumstances are present, the DOJ may still choose to decline prosecution based on an analysis of the severity of the circumstances weighed against the company's cooperation and remedial efforts. The DOJ will require the company to pay all disgorgement, forfeiture, restitution, and victim compensation as part of the declination agreement.
- The Criminal Division will provide a Non-Prosecution Agreement ("NPA") where a company has fully cooperated and implemented timely and appropriate remedial measures but is ineligible to receive a declination of prosecution because it (1) submitted a good faith disclosure that does not qualify as a VSD or (2) where aggravating factors are present. The NPA shall:
 - Have a term length of less than three years;
 - Not require the company to maintain an independent compliance monitor;
 - Provide for a 75% reduction off the low end of the sentencing guidelines range for any criminal fine that is imposed.
- In the event that a company does not qualify for a declination of prosecution or NPA as described above but has satisfied some cooperative or remedial elements, the DOJ will recommend up to a 50% reduction off the low end of the sentencing guidelines range.
- A guilty plea is generally not required unless there are particularly egregious or multiple aggravating circumstances.
- A monitor requirement depending on the facts and circumstances of a case (unless company has implemented an effective compliance program).

Note that on June 9, 2025, the Deputy Attorney General issued a memorandum to the Criminal Division on "Guidelines for Investigations and Enforcement of the Foreign Corrupt Practices Act (FCPA)." Though not focused on VSDs, these

guidelines offer insights into the DOJ's enforcement priorities that are important for companies to consider when weighing the potential risks and benefits of voluntarily disclosing FCPA violations. The points below outline the enforcement priorities and factors Criminal Division prosecutors are directed to consider when determining whether to investigate and prosecute FCPA violations.

- Whether the subject misconduct relates to the criminal operations of Cartels and Transnational Criminal Organizations ("TCOs"), money laundering activity for Cartels or TCOs, or is linked to state employees or foreign officials that have received bribes from Cartels or TCOs;
- Whether the subject misconduct had negatively impacted the ability of an identifiable American business or person to have fair access to or compete in a foreign market or resulted in an economic injury;
- The extent to which alleged misconduct involves routine business practices in foreign countries and prioritizing cases involving corrupt intent that can be tied to particular individuals, substantial bribe payments, and schemes to conceal bribery or other fraudulent conduct.

F. Department of Justice, National Security Division ("NSD"), Enforcement Policy for Business Organizations

The DOJ's NSD is responsible for overseeing cases that implicate U.S. national security, including those that involve violations of U.S. export controls and economic sanctions.

1. Voluntary Self-Disclosure

- To receive full credit under the NSD's policy, a company must (1) submit a VSD to the NSD, (2) fully cooperate, and (3) timely and appropriately remediate the violations.
- A disclosing party may not receive credit under this policy if it submits a voluntary disclosure only to regulatory agencies such as BIS, DDTC, or OFAC, rather than the NSD. However, a disclosing party may still qualify for credit under this policy where it has voluntarily disclosed misconduct in good faith to another DOJ office or component and the NSD is involved in the resolution.
- A VSD must be submitted to the NSD "within a reasonably prompt time" after the company becomes aware of the misconduct and "prior to an imminent threat of disclosure or government investigation."
- A VSD must contain all relevant facts known to the company at the time of the disclosure, including the identity of individuals substantially involved in, or responsible for, the misconduct.
- Full cooperation requires timely disclosure (within the VSD or via subsequent updates to the NSD) of all non-privileged facts relevant to the misconduct at issue, including:

- All relevant facts gathered during a company's independent investigation;
 - Attribution of facts to specific sources where such attribution does not violate the attorney-client privilege, rather than a general narrative of the facts;
 - Timely updates on a company's internal investigation, including but not limited to rolling disclosures of information;
 - All facts related to involvement in the criminal activity by the company's officers, employees, or agents;
 - All facts known or that become known to the company regarding potential criminal conduct by all third-party companies; and
 - Identification of all individuals involved in or responsible for the misconduct at issue, regardless of their position, status, or seniority, including the company's officers, employees, customers, competitors, or agents and third parties, and all non-privileged information relating to the misconduct and involvement by those individuals.
- Witnesses for interviews (and deconfliction of witness interviews), production of documents, including overseas documents, and employees and agents may be required.
 - The VSD should include a description and timeline of the steps the company is taking to remediate the disclosed misconduct, including a root cause analysis, outline of the implementation or enhancement of a compliance and ethics program, and an overview of disciplinary actions that were taken.
 - Aggravating factors include: exports of items controlled for nuclear nonproliferation or missile technology reasons to a proliferator country; exports of items known to be used in the construction of weapons of mass destruction; unlawful transactions or exports to Foreign Terrorist Organizations or Specially Designated Global Terrorists; exports of military items to a hostile foreign power; repeated violations of U.S. national security laws, including similar administrative or criminal violations in the past; a significant profit obtained by the company due to the misconduct; sanctions or export offenses that are actively concealed by other serious criminal activity such as fraud, or corruption; and concealment or involvement of upper management in the criminal conduct.

2. VSD Submission

The Enforcement Policy for Business Organizations notes that VSDs covered under the Policy should be emailed to NSD.VSD@usdoj.gov.

3. Potential Action by DOJ

- There will be a presumption that a disclosing company will receive an NPA and no fine where such company submits a VSD to the NSD, fully cooperates with the NSD's investigation, implements timely and appropriate remedial measures, and where no aggravating factors are present.
- The NSD has the discretion to decline prosecution when warranted under the principles of federal prosecution.
- A guilty plea or deferred prosecution agreement ("DPA") may be required

when aggravating factors are present. However, where a company has submitted a VSD, fully cooperated, and implemented remedial measures, fines assessed against the company will be capped at an amount equal to the gross gain or loss.

- Parties can still possibly gain an NPA in the face of aggravating factors if the prosecutor determines it to be the appropriate outcome following an assessment of the severity and prevalence of the aggravating circumstances and the level and degree of the company's cooperation.
- A monitorship will generally not be required where the company demonstrates that it has implemented and tested a well-designed and effective compliance program as well as taken appropriate steps to remediate the underlying cause of the misconduct at the time of resolution.
- Companies will be responsible for disgorgement, forfeiture, and/or restitution resulting from the misconduct at issue.

G. Department of Justice, Commercial Litigation Branch, Guidelines for Taking Disclosure, Cooperation, and Remediation into Account in False Claims Act Matters

The DOJ's Commercial Litigation Branch is responsible for the investigation and prosecution of cases involving fraud against the U.S. government. The Fraud Section within the Commercial Litigation Branch, in coordination with U.S. Attorney's Offices, may pursue civil remedies under the federal False Claims Act ("FCA") (31 U.S.C. § 3729) in cases involving violations of U.S. trade and national security laws, including customs violations.

1. Voluntary Self-Disclosure

- To make an effective self-disclosure that qualifies for credit, a company must make a timely, proactive, and voluntary self-disclosure to the DOJ.
- Additional credit may be given if a company discloses other misconduct discovered during an internal investigation after an initial disclosure has already been made.
- Credit may also be given to companies that cooperate with an ongoing DOJ investigation. Cooperation may include:
 - Identifying individuals substantially involved in the misconduct;
 - Continuously reporting relevant facts or other information to the DOJ;
 - Preserving, collecting, and disclosing relevant documents and information that goes beyond existing business practices or legal requirements;
 - Ensuring company officers and employees are available for interviews or meetings with the DOJ as necessary;
 - Disclosing findings discovered during the company's independent internal investigation;
 - Providing information on potential misconduct and involvement of third parties;
 - Admitting liability and assisting in the determination or recovery of losses caused by the underlying misconduct.

- The DOJ will consider the following when determining the value of VSDs and other forms of cooperation:
 - The cooperation's timeliness and voluntariness;
 - The truthfulness, completeness, and reliability of any information or testimony provided;
 - The extent and nature of the assistance; and
 - The cooperation's significance and usefulness.
- DOJ attorneys will also take into account remedial measures enacted by a company following an FCA violation.

2. VSD Submission

In general, a VSD may be submitted to different DOJ offices or components based on the underlying facts of a potential violation and matter type. The FCA VSD guidelines do not provide specific instructions on how to submit a VSD to the DOJ for credit under this policy. A disclosing party should consult legal counsel and relevant DOJ website pages, including the local U.S. Attorney's Office page to identify the appropriate DOJ contact.

3. Potential Action by DOJ

- To receive maximum credit under this policy, a company must (1) submit a VSD to the DOJ, (2) fully cooperate, and (3) timely and appropriately remediate the violations. Partial credit may be given where a company has meaningfully assisted the government's investigation.
- Credit will likely be in the form of reducing the amount of penalties or damages multiple sought by the department. However, the DOJ will not award credit exceeding an amount that would result in the government not receiving full compensation for the losses incurred.
- The DOJ will not award credit if a company acts with a lack of good faith toward the government during its investigation or hides involvement in the misconduct by members of senior management or the board of directors.
- The DOJ retains discretion when rewarding credit. Additionally, the value of the credit a company receives will depend on underlying facts and circumstances of the case.
- When appropriate, the DOJ may consider additional avenues that would permit an entity or individual to claim credit in FCA cases, including:
 - Notifying a relevant agency about a company's disclosure, other cooperation, or remediation so that the DOJ in its discretion may consider such factors in evaluating its administrative options, such as suspension or civil monetary penalty decisions;
 - Publicly acknowledging a company's disclosure, other cooperation, or remediation; and
 - Assisting a company in resolving qui tam litigation with a relator or relators.

H. Department of Justice, U.S. Attorney's Offices ("USAO"), Voluntary Self Disclosure Policy

This policy sets a nationwide standard for all USAOs. A company may choose to

submit a VSD of criminal conduct to any USAO. If another DOJ component is involved in prosecuting the case, or if the violations are covered by another DOJ component's VSD policy, the USAO will coordinate with the relevant DOJ component and may apply a provision of an alternate VSD policy when necessary.

1. Voluntary Self-Disclosure

- A VSD must be voluntary and cannot be made pursuant to a preexisting obligation to disclose.
- A VSD must be made "within a reasonably prompt time" after the company becomes aware of the misconduct and "prior to an imminent threat of disclosure or government investigation."
- A VSD must contain all relevant facts known to the company at the time of the disclosure. If certain relevant facts are not known at the time of disclosure, the disclosing party should state that its disclosure is based on a preliminary investigation or assessment. If an internal investigation is conducted, the disclosing party should provide factual updates to the USAO as the investigation progresses.
- A company should move in a timely fashion to preserve, collect, and produce relevant documents and factual information to the USAO.
- The VSD should include timely measures taken by the company to remediate the criminal conduct, including the implementation or enhancement of a compliance program.
- Aggravating factors include misconduct that poses a grave threat to national security, public health, or the environment; the presence of deeply pervasive misconduct throughout the company; and/or executive management involvement in the misconduct.

2. VSD Submission

In general, a VSD may be submitted to the U.S. Attorney's Office in the district where the misconduct occurred. The USAO VSD Policy does not provide specific instructions on how to submit a VSD to a USAO. A disclosing party should consult the relevant USAO's website to find contact information for the office.

3. Potential Action by DOJ

- Declination, Non-Prosecution Agreement, or Deferred Prosecution Agreement (absent aggravating factors).
- Guilty plea with reduced fines (when aggravating factor(s) is present).
- Reduced fines, or, in some cases, no issuance of fines.
- Monitor requirement (unless company has implemented an effective compliance program).
- Companies will be responsible for disgorgement, forfeiture, and/or restitution resulting from the misconduct at issue.

I. Department of Justice, Mergers & Acquisitions Safe Harbor Policy

Announced on October 4, 2023, this policy sets Department-wide standards for voluntary disclosures in the mergers and acquisitions ("M&A") context. Under this policy, an acquiring company may receive a presumption of declination when it discloses misconduct discovered at an acquired entity within the Safe Harbor period, cooperates with the related investigation, and takes timely remedial measures. The

implementation of this policy may differ between the various DOJ components. However, each DOJ component will apply the policy consistent with the following points:

- Companies must disclose misconduct discovered at an acquired entity within six months of the closing date regardless of whether the misconduct is discovered before or after the acquisition.
- Companies will have one year from the date of closing to fully remediate the reported misconduct.
- The deadlines for disclosure and remediation are subject to a reasonableness analysis and may be extended by the DOJ depending on the facts or circumstances of a specific case.
- Aggravating factors present at the acquired company will not affect the acquiring company's ability to receive a declination. In addition, misconduct disclosed by an acquiring company under this policy will not be treated as past violation in any future recidivist analysis for the acquiring company.

J. Department of Homeland Security, U.S. Customs and Border Protection

CBP is responsible for enforcing the import laws of the United States.

1. Prior Disclosure ("PD") 19 U.S.C. § 1592(c)(4) / 19 C.F.R. § 162.74

Information marked with an asterisk (*) can be found in CBP Directive No. 5350-020A, Processing Prior Disclosure Submissions. This Directive serves as internal guidance for relevant CBP offices and suggests a policy toward the standardization of PD practices throughout CBP offices.¹

- A valid PD must be submitted to CBP before, or without knowledge of, the commencement of a formal investigation by CBP, ICE, or Homeland Security Investigations ("HSI").
- A PD discloses the circumstances of a violation of 19 U.S.C. § 1592, which prohibits the entering of merchandise into the commerce of the United States through fraud, gross negligence, or negligence resulting in a material and false statement or a material omission.
 - Examples of 19 U.S.C. § 1592 violations include incorrect valuation, misdescription of merchandise, misclassification, evasion of antidumping/countervailing duty orders, improper country of origin declarations or markings, or improper claims for preferential tariff treatment under a free trade agreement or other duty preference program.
- A valid PD reduces penalties for 19 U.S.C. § 1592 violations.
- A PD may be submitted by any party involved in the business of importing into the United States, including but not limited to importers, customs brokers, exporters, shippers, and foreign suppliers/manufacturers.
- The disclosing party must tender the duty loss to CBP for the PD to be considered valid if the PD involves duty loss violations.
 - Disclosing parties may make tender at the time of PD submission, or within 30 days after the party is notified by CBP of the amount to be

¹ Directives issued by CBP do not change PD requirements listed in 19 U.S.C. § 1592(c)(4) or 19 C.F.R. § 162.74; however, the noted Directive provides helpful insight into the logistics and internal practices related to PD submissions.

- tendered;
 - CBP personnel will forward payments made with submissions of PD to local cashier within two days of receipt;*
 - Cashier will deposit payment within one day after receipt of payment and will send notification of deposit to the disclosing party;*
- Four elements must be included in a PD submission:
 - The type of merchandise involved;
 - The entry number, or each relevant Customs port and the approximate entry dates;
 - The materially false statements, omissions, or acts, and an explanation of how they occurred; and
 - The true information that should have been provided instead of the materially false or omitted information.
- The disclosing party must provide any information unknown at the time of the PD submission within 30 days of the initial disclosure date. Extensions of the 30-day period may be requested by the disclosing party from the concerned Fines, Penalties, and Forfeitures officer. No more than one period of 60 business days shall be granted as an extension to perfect a PD.*

2. PD Submission

PDs may be submitted to the appropriate CBP Center for Excellence and Expertise (“CEE”) or any port of entry where the disclosed violation occurred. If violations occurred at multiple ports of entry, the disclosing party should list all affected ports in the PD. The PD should be addressed to the Commissioner of CBP and have the words “Prior Disclosure” conspicuously printed on the face of the envelope.

If the PD is submitted via registered or certified U.S. Mail, return-receipt requested, the PD shall be deemed to have been made at the time of mailing. If the PD is submitted by any other method, the PD will be deemed to have been made at the time of receipt by CBP. PDs can now also be submitted via email to the relevant point of contact at the CEE or to Fines, Penalties, and Forfeitures.

3. Potential Action by CBP

- CBP will review a PD submission and inform the disclosing party whether the PD is valid or invalid.
 - If the PD is valid, CBP will issue a request for payment of the mitigated penalty amount, if applicable.
 - If the PD is not valid on the basis of a formal investigation commenced prior to the PD submission, CBP will commence a penalty proceeding under 19 U.S.C. § 1592.
 - Offsetting will not be allowed where the disclosing party (i) has overpaid as a result of failure to establish a duty allowance or preference; (ii) a § 1592 violation was made knowingly or intentionally; or (iii) where overpayment was made to violate a law.
 - A PD that attempts to apply offsetting will be referred to Regulatory Audit and Agency Services (“RAAAS”)² for audit. An offsetting determination will be communicated to the disclosing party at the time

² RAAAS is comprised of field offices throughout the United States that provide auditing services in collaboration with U.S. Customs and Border Protection. The audits generally focus on compliance, a violation, or specific concerns raised by CBP. RAAAS audits are typically initiated via a referral by CBP.

of the PD acceptance or denial decision;*

- Under a valid PD, the penalty reduction is different depending on the whether the violation involved negligent, grossly negligent, or fraudulent conduct.
 - For fraudulent violations with a PD, the penalty shall not exceed (1) an amount equaling 100% of the lawful duties, taxes, and fees of which the U.S. is deprived, or (2) 10% of dutiable value if the violation did not affect duty assessment.
 - For negligent and grossly negligent violations with a PD, the penalty shall not exceed the interest on the amount of lawful duties, taxes, and fees.
- For criminal violations, CBP is legally obligated to refer the information to the U.S. Attorney's Office, which will make a decision on whether or not to prosecute the alleged criminal violation.
- CBP may find no violation of 19 U.S.C. § 1592.



TORRES TRADE LAW

INTERNATIONAL TRADE & NATIONAL SECURITY

Questions? Contact Us:

Call 202.851.8200 or 214.295.8473

Email Info@torrestradelaw.com

Sign up for our newsletter: www.torrestradelaw.com