



TORRES TRADE LAW

INTERNATIONAL TRADE & NATIONAL SECURITY



Voluntary Self-Disclosure Handbook

November 17, 2022 | 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. Initial Notification 15 C.F.R. § 764.5(c)(2)
 - 2. Extensions of Time to Submit Final Narrative Account 15 C.F.R. § 764.5(c)(2)(iv)
 - 3. Final Narrative Account 15 C.F.R. § 764.5(c)(3)
 - 4. VSD Submission
 - 5. 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 Fraud Section, Foreign Corrupt Practices Act (“FCPA”) Corporate Enforcement Policy
 - 1. Voluntary Self-Disclosure
 - 2. VSD Submission
 - 3. Potential Action by DOJ
- F. Department of Justice, National Security Division (“NSD”), Export Control and Sanctions Enforcement Policy for Business Organizations
 - 1. Voluntary Self-Disclosure
 - 2. VSD Submission
 - 3. Potential Action by DOJ
- G. 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 or export 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 the full 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 can have a number of benefits with respect to reducing the likelihood and severity of monetary fines and administrative actions by regulators in the event of the discovery of violations as well as establish a positive relationship with such regulators in the event of any future regulatory issues. A VSD can:

- 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.
- Act as a mitigating factor when determining the amount and severity of penalties for violations.

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 potentially improper conduct.
- Criminal violations may be referred to the U.S. Department of Justice (“DOJ”) for prosecution.
- A VSD creates knowledge of violations, which could create liability should “knowing” violations occur after disclosure.
- A VSD can lead to loss of confidentiality.
- Regulatory authorities may require waiver of certain defenses or extension of time period (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).

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 litigations, 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 than 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; 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”); and the U.S. Department of the Treasury, Office of Foreign Assets Control (“OFAC”).

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”).

It should also be noted that DOJ has created a parallel voluntary disclosure program permitting submission of voluntary self-disclosures directly to the DOJ for potential criminal violations of the export control and sanction laws. DOJ has indicated that such disclosure may “significantly” reduce criminal penalties, including “a non-prosecution agreement (“NPA”), 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, BIS

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

1. Initial Notification 15 C.F.R. § 764.5(c)(2)

The Initial Notification should be made to BIS, Office of Export Enforcement (“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.
- 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. Final narrative account is due 180 days from OEE’s receipt of the Initial Notification.

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

OEE can grant an extension at its discretion. In order to be considered, a request must show:

- Review was started promptly after discovery of violations.
- 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; designate a contact person and provide contact person’s business address, email address, and telephone number; and provide additional information that person making the request reasonably believes is pertinent.

3. Final Narrative Account 15 C.F.R. § 764.5(c)(3)

After the Initial Notification, a thorough review should be conducted 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 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.
- 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—as described in more detail below, 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(c)(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(c)(5)**
 - Must certify that all of the representations made in connection with the VSD are true and correct to the best of person's knowledge and belief.
- **Oral Presentations § 764.5(c)(6)**
 - An oral presentation to OEE can be requested but is not necessary.

4. VSD Submission

VSDs must be submitted to:

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

5. Potential Action by OEE 15C.F.R. § 764.5(d)

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

- Take no action;
- Issue a warning letter;
- Issue a proposed charging letter and attempt to settle;
- Issue charging letter (if settlement not reached);
- Administrative actions, including denial of, or restriction on, export/import privileges; and/or
- Refer to DOJ for criminal prosecution (rare in VSD cases).

It should be noted that on June 30, 2022, OEE announced policy changes relating to VSDs. The policy updates suggest a shift toward more uniform methods of designating certain violations as “egregious” and thus qualifying them for stiffer penalties. Additionally, the new policies encourage efficiency within the VSD process. Specifically, voluntary disclosures of minor or “technical” violations will now be fast-tracked with letters of warning or no-action being issued within 60 days of final disclosure. More serious VSD cases will be assigned a field agent and OCC attorney to follow up with the disclosing party.

B. U.S. Department of State, DDTC

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 (will be similar in scope to that described for disclosures to the Department of Commerce, 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 systematic 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);
- Referral to DOJ for criminal prosecution (rare in VD cases).

C. U.S. Department of Commerce, Census

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 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)

- Review period should cover a period of five years prior to date of the Initial Notification.
- Narrative must sufficiently describe nature and gravity of suspected violations; must also include nature of review conducted and measures taken to minimize the likelihood of future violations.
- Additionally, the narrative should include:
 - Type(s) of violation involved;
 - Describe 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.

4. VSD Submission

VSDs may be submitted electronically by emailing a password-protected file to emd.askregs@census.gov or by secure fax at 301-763-8835. VSDs may also be submitted by delivery to the address below:

Chief, Economic Management Division
U.S. Census Bureau
4600 Silver Hill Road, Room 6K064
Suitland, MD 20746 (if sent by courier) or Washington, D.C. 20233 (if sent by mail)

5. Potential Action by Census 15C.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 will notify CBP, Immigration and Customs Enforcement (“ICE”), and OEE of the VSD and will 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, OFAC

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 period, 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 Fraud Section, Foreign Corrupt Practices Act (“FCPA”) Corporate Enforcement Policy

1. Voluntary Self-Disclosure

A company can choose to submit a VSD for violations of the FCPA to the DOJ’s Criminal Division Fraud Section.

- 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.
- A VSD should timely disclose all relevant facts and documents, 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.
- Production of documents, witnesses for interviews, including overseas documents and employees and agents may be required.
- The VSD should include remediation steps including a root cause analysis, implementation or enhancement of a compliance and ethics program, and disciplinary measures.
- Submission of VSD will result in presumption that the company will receive a declination absent aggravating circumstances.
- 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:

Deputy Chief (FCPA Unit), Fraud Section, Criminal Division
 Bond Building
 1400 New York Avenue, N.W.
 Washington, D.C. 20005
 Phone: 202.514.7023; Email: fcpa.fraud@usdoj.gov

3. Potential Action by DOJ

- Declination of prosecution of the company (regardless of the criminal resolution, companies are still required to disgorge profits tied to the misconduct).
- In the event that a criminal fine is imposed, DOJ will recommend a 50 percent reduction off the bottom end of the sentencing guidelines for self-disclosing parties.
- DOJ could still go after individual wrongdoers.

F. Department of Justice, National Security Division (“NSD”), Export Control and Sanctions Enforcement Policy for Business Organizations

The DOJ NSD’s Counterintelligence and Export Control Section (“CES”) oversees criminal violations related to U.S. export controls and sanctions.

1. Voluntary Self-Disclosure

- A VSD must be submitted to the NSD’s CES at substantially the same time as VSDs are submitted to DDTC, BIS, or OFAC.
- 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.
- A VSD should timely disclose all relevant facts and documents, 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.
- 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 remediation steps including a root cause analysis, implementation or enhancement of a compliance program, and disciplinary measures.
- 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; exports to Foreign Terrorist Organizations or Specially Designated Global Terrorists; exports of military items to a hostile foreign power; repeated violations, including similar administrative or criminal violations in the past; and knowing involvement of upper management in the criminal conduct.

2. VSD Submission

The Export Control and Sanctions Enforcement Policy for Business Organizations notes that VSDs covered under the Policy should be emailed to NSDCES.ExportVSD@usdoj.gov. VSDs can also be delivered by mail to the address listed below:

Deputy Chief for Export Control and Sanctions
Counterintelligence and Export Control Section
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

3. Potential Action by DOJ

- Non-Prosecution Agreement and no fines (absent aggravating factors).
- Deferred Prosecution Agreement or guilty plea;
- Issuance of reduced 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.

G. Department of Homeland Security, U.S. Customs and Border Protection¹

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

- 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 party may make tender at the time of PD submission, or within

¹ 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 and suggests a policy toward the standardization of PD practices throughout CBP offices. 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.

- 30 days after the party is notified by
 - CBP of the amount to be tendered;
 - CBP personnel will forward payments made with submissions of PD to local cashier within 2 days of receipt*;
 - Cashier will deposit payment within 1 day after receipt of payment and will send notification of deposit to 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 1 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 a number of 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.

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 over-payment 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 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.

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 from CBP.



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