

**DEFENSE TRADE ADVISORY GROUP**  
**Trade Compliance Process Working Group**  
**White Paper**

**Tasking**

The June 30, 2015 tasking letter from the Deputy Assistant Secretary of State for Political-Military Affairs assigned the Defense Trade Advisory Group (DTAG) to review and comment on four issues. Working Group 1 analyzed the Trade Compliance Process, specifically:

Review the current Voluntary Disclosure (VD) process and provide recommendations for how to ensure that foreign policy and national security interests are given greater focus in the preparation, review, and adjudication process. Specifically, (a) analyze how to address “administrative” VDs, including how to distinguish “administrative” VDs from other VDs and whether a “binning” or triage process would be beneficial both to the Directorate of Defense Trade Controls and industry; (b) review the Department of State’s approach to regulatory enforcement versus the Department of Commerce’s approach and analyze how or if the approaches could be synchronized and/or modified; (c) consider whether VD policies or procedures from other regulatory agencies may have elements that could be of benefit for State; and (d) review how the trade compliance process may need to change if/when State and Commerce’s trade regulatory bodies merge in the future.

**Working Group Members**

Dava Casoni  
Monica Chavez  
Giovanna Cinelli  
Mike Cormaney, Co-Chair  
Greg Creeser  
B.J. Demery  
Larry Dodson  
Matthew Goldstein  
Cynthia Keefer, Co-Chair  
Spence Leslie  
Christine McGinn  
Joy Robins  
Joe Veiga

## **Approach**

The DTAG's charter is to provide recommendations to the Assistant Secretary for Political-Military Affairs with regard to regulatory and policy changes managed by the Department of State (DoS), Directorate of Defense Trade Controls (DDTC). The Trade Compliance Process Working Group (WG) focused on DoS issues; however, this tasking stated specifically for the DTAG to consider, compare and recommend potential regulatory and policy changes managed by the Department of Commerce (DoC).

The WG first gathered relevant information from DTAG members, industry participants, law firms, consulting firms, non-profit companies, and universities. Additionally, the WG reviewed the standards employed by other government agencies. For example, the standard used by the National Industrial Security Program (NISP) regarding the loss, compromise or suspected compromise of classified information.<sup>1</sup> Based on the information gathered, the WG then developed a baseline approach to address each of four elements of the assigned tasking.

## **Existing Policy & Regulatory Environment**

In accordance with the International Traffic in Arms Regulations (ITAR), disclosures are voluntary except that a person is required to immediately inform DDTC if the person "knows or has reason to know of a proposed, final, or actual sale, export, transfer, reexport, or retransfer of articles, services, or data" involving a country or national identified in 22 C.F.R. §126.1.<sup>2</sup> Disclosures under the Export Administration Regulations (EAR) are generally voluntary.<sup>3</sup>

There are additional circumstances where disclosures under the ITAR or the EAR may be required, such as correcting or supplementing information previously submitted to the relevant agency or disclosing information relevant to decision makers in the submission of authorization requests.<sup>4</sup> The purpose of this document is to discuss the WG recommendations and not to provide legal guidance on when disclosures are otherwise required under the ITAR or EAR.

The WG is not recommending any changes to the mandatory disclosure requirement under 22 C.F.R. §126.1(e)(2) or to the otherwise voluntary nature of disclosures under the ITAR and EAR.

---

<sup>1</sup> Section 1-303 of the National Industrial Security Program Manual, DoD 5220.22-M (Mar. 28, 2013) (stating "Any loss, compromise or suspected compromise of classified information, foreign or domestic, shall be reported to the CSA. Classified material that cannot be located within a reasonable period of time shall be presumed to be lost" until an investigation determines otherwise).

<sup>2</sup> 22 C.F.R. §126.1(e)

<sup>3</sup> 15 C.F.R. § 764.5

<sup>4</sup> Disclosure requirements incorporated into Consent Agreements are outside the scope of this white paper.

## Assumptions

1. In the absence of empirical data (metrics), this WG has based its recommendations on the implied objective of the DoS to focus compliance resources where they will be the most needed and most effective in addressing U.S. national security and foreign policy interests.
2. Further, Export Control Reform (ECR) prompted significant changes in the scope of the ITAR. The intent was for the revised U.S. Munitions List (USML) to have a more targeted focus on those items and technologies that are most sensitive, the export of which are most likely to implicate national security and foreign policy considerations.
3. The WG recognizes that industry is not in a position to fully assess the national security or foreign policy implications of ITAR violations as this is exclusively a U.S. Government role.

## Key Terms & Elements

Several key terms in the tasking are not defined within the ITAR or the EAR. For example, “administrative” is used in the tasking letter to identify a class of violations of ITAR requirements. The WG discussed the various meanings of the term “administrative” and possible alternative wording, such as “process-related”; however, the WG adopted the term “administrative” as it was used in the tasking.

Absent a regulatory definition, the WG adopted the plain and ordinary meaning<sup>5</sup> of the words as follows:

- Administrative: the activities that relate to the management of an operation such as a company or government; to manage, keep track of, take care of records and documents
- Binning: to place a thing in an enclosed place for storage or to place into a category for organizational purposes
- Category: any of several fundamental and distinct classes to which entities or concepts belong
- Triage: the sorting of and allocating of tasks according to the priority of the matter so that resources are positioned where they can be best used, are most needed, or most likely to achieve success

This WG also identified key characteristics for any proposed methodology to identify what constitutes an “administrative” violation. The methodology should be objective, straightforward (*i.e.*, easy to understand and administer), flexible (*i.e.*, able to account for changes in underlying facts and circumstances), and contain consequences for improper implementation of the recommended solution.

---

<sup>5</sup>See *FDIC v. Meyer*, 510 U.S. § 471, 476 (1994) (“In the absence of such a definition, [courts] construe a statutory term in accordance with its ordinary or natural meaning.”).

## Discussion

- a. *Analyze how to address “administrative” VDs, including how to distinguish “administrative” VDs from other VDs and whether “binning” or triage process would be beneficial both to the Directorate of Defense Trade Controls and industry;*

The WG considered the following four options before arriving at our recommended methodology:

- Borrow the standard implemented by the National Industrial Security Program (NISP)
- Designate specific ITAR provisions as “administrative”
- Classify violations by their severity/level of risk using a risk matrix
- Review aggravating and mitigating factors to identify potentially less serious violations

Following is a discussion of each of the options listed above.

### Option 1: Analogizing to the NISP Standard

The NISP defines the types of violations that must be reported to the cognizant U.S. Government agency as those that involve either loss, compromise, or suspected compromise of classified information. Violations of other security requirements are not reportable, which indicates that they are not as significant to the cognizant agency from a national security or foreign policy perspective.

Using this same concept, an “administrative” violation of the ITAR would be one that does not involve (a) the loss, compromise or suspected compromise of a Defense Article (including Technical Data) or (b) the performance of a Defense Service (which, by definition, involves the furnishing of assistance to a foreign person).

This standard is objective as actual release of items or technologies which are most likely to impact national security and/or foreign policy interests has occurred. The initial analysis does not require a review of what was lost, to whom, and so forth – the only standard is whether Defense Articles (including Technical Data) were released or Defense Services were provided. Further, the NISP standard is included in established regulations with a history of implementation that may be referenced with definitions that may be adopted.

It is also worth noting that protection of Defense Articles under the NISP requires an organization and appropriate subject matter experts to implement a comprehensive risk management system. This entails training, threat and risk awareness, knowledge of safeguarding requirements, internal controls, self-audits, reporting, accountability, and so forth. The management system requirements are similar in scope to best practices needed for ITAR compliance.

### Option 2: Classifying by ITAR Provisions

This approach sought to designate specific ITAR provisions as “administrative.” ITAR provisions were reviewed individually and were categorized as either “administrative” or non-“administrative.” The candidates for administrative violations included requirements such as (a) submitting a copy of a signed Agreement within thirty days of execution<sup>6</sup> or (b) notifying DDTC within 60 days of an impending termination of an Agreement.<sup>7</sup>

While this approach was objective and straightforward, the categorization of each provision was fraught with unknown enforcement variables. In addition, there was limited flexibility in this approach. Circumstances may exist where a process-related provision may implicate national security or foreign policy considerations (*e.g.*, intentional decision to not maintain records or to destroy records where both are related to activities subject to the ITAR). In the alternative, a non-administrative ITAR violation may occur where there is little – if any – potential harm to national security or foreign policy interests (*e.g.*, unauthorized export of a part to a NATO<sup>8</sup> ally for which there are multiple precedent cases for the same item, end user and program).

### Option 3: Risk Matrix

Under this approach, a graphical methodology is employed to identify, assess, and assign a level of risk to potential ITAR violations. This method is similar to what is currently utilized generally in the informational technology industry and in the Department of Defense’s procurement process.

A risk matrix (*see Exhibit 1*) could classify violations by (a) Level of Magnitude (ranging from Level 1 to Level 4 in terms of impact on national security/foreign policy) and (b) Rate of Occurrence (or probability), ranging from Certain to Rare.

---

<sup>6</sup> 22 C.F.R. §124.4(a)

<sup>7</sup> 22 C.F.R. §124.6

<sup>8</sup> Additional information regarding the North Atlantic Treaty Organization (NATO) is available at: <http://www.nato.int>.

**Exhibit 1**

		Level of Magnitude: Impact on National Security/Foreign Policy			
		Level 1	Level 2	Level 3	Level 4
Rate of Occurrence: Probability	CERTAIN	Annual Report	Semi-Annual Report	Semi-Annual Report	Monthly
	LIKELY	Annual Report	Monthly	Monthly	Immediately
	POSSIBLE	Semi-Annual Report	Monthly	Immediately	Immediately
	UNLIKELY	Semi-Annual Report	Monthly	Immediately	Immediately
	RARE	Monthly	Immediately	Immediately	Immediately

Where a violation is located within the matrix would determine the consequences for the violation and whether it was viewed as “administrative.” For example, a violation which was determined to be “Certain” to occur (*i.e.*, common) and a magnitude of “Level 1” would be viewed as “administrative” in nature eligible for an annual consolidated reporting option. In contrast, a violation that is “Rare” (*i.e.*, uncommon) and that is “Level 4” would not be deemed as “administrative.”

This approach is highly dependent upon facts and circumstances. The WG determined that it was too subjective for practical application with regard to ITAR violations as industry does not have the ability to access the information necessary to make assessments regarding the magnitude of a violation’s impact on national security or foreign policy. In addition, potential incongruity or disagreements between industry and DDTC regarding magnitude determinations would be likely.

*Option 4: Review of Aggravating & Mitigating Factors*

This methodology would identify “administrative” violations by reviewing a list of aggravating and mitigating factors for each potential violation. A list of potential aggravating or mitigating factors is provided below in **Exhibit 2**. These factors are examples that were derived from published DoS consent agreements, other agency enforcement guidelines (*e.g.*, the Bureau of Industry and Security, Office of Foreign Assets Control), and the Department of Justice’s sentencing guidelines.

## Exhibit 2

AGGRAVATING	FACTOR	MITIGATING
<ul style="list-style-type: none"> <li>• 126.1 issues or “ineligible” parties</li> <li>• Implicates reason for control</li> </ul>	Destination & Parties	<ul style="list-style-type: none"> <li>• “Friendly” countries</li> <li>• Unrelated to reason for control</li> </ul>
<ul style="list-style-type: none"> <li>• None (or RWAs/denials)</li> </ul>	Precedent Approval(s)	<ul style="list-style-type: none"> <li>• Multiple – for same country/end user</li> </ul>
<ul style="list-style-type: none"> <li>• Repetitive violations of same type</li> <li>• Systemic issues</li> <li>• Intentional/willful action</li> </ul>	Nature of Violation(s)	<ul style="list-style-type: none"> <li>• Isolated incident</li> <li>• No willful/intentional conduct</li> <li>• Small quantity/value of exports</li> </ul>
<ul style="list-style-type: none"> <li>• Continuing conduct</li> <li>• Failure to identify in timely manner</li> </ul>	Corrective Actions	<ul style="list-style-type: none"> <li>• Effective actions implemented</li> <li>• Item/technology retrieved</li> </ul>
<ul style="list-style-type: none"> <li>• Attempt to hide/conceal violations</li> </ul>	Cooperation	<ul style="list-style-type: none"> <li>• VD/alternative process</li> <li>• Respond fully in a timely manner</li> </ul>
<ul style="list-style-type: none"> <li>• Lack of support</li> <li>• Ineffective resources allocated</li> </ul>	Management Support	<ul style="list-style-type: none"> <li>• Full support</li> <li>• Adequate personnel &amp; resources available</li> </ul>
<ul style="list-style-type: none"> <li>• Sensitive (e.g., MTCR, SME)</li> <li>• Manufacturing “know how”</li> </ul>	Items/ Technology Involved	<ul style="list-style-type: none"> <li>• Less sensitive (e.g., parts/components)</li> <li>• No knowledge transfer (e.g., “build to print”)</li> </ul>

When applying this approach to a potential violation the WG determined that, like the Risk Matrix, it was too subjective and too flexible to produce a consistent result.

### Proposed Methodology

Based on the discussion above, the WG developed a methodology (summarized in **Exhibit 3**) that combines the best and most useful elements of each option reviewed.

## Exhibit 3

CATEGORY	DESCRIPTION	PRESUMED CONSEQUENCES
<b>1</b>	Involves: 1. 126.1 country/national; <u>and</u> 2. One of the following: (a) Loss or compromise; (b) Performance of Defense Service; <u>or</u> (c) Proposal/presentation to sell, export, re-export, etc.	<ul style="list-style-type: none"> <li>• “Immediate” disclosure mandatory under 126.1(e)</li> <li>• Presumption not rebuttable by mitigating factors</li> </ul>
<b>2</b>	Involves: 1. Countries/nationals other than 126.1; <u>and</u> 2. Loss or compromise or performance of Defense Service	<u>IF</u> decision made to disclose: <ul style="list-style-type: none"> <li>• Existing 127.12 process</li> <li>• Presumption rebuttable by aggravating/mitigating factors</li> </ul>
<b>3</b>	<u>No</u> loss or compromise or Defense Service	<u>IF</u> decision made to disclose: <ul style="list-style-type: none"> <li>• Options for alternatives to 127.12</li> <li>• Presumption rebuttable by aggravating/mitigating factors</li> <li>• <u>Note:</u> Proposals/presentations involving 126.1 countries with no loss/compromise still Category 1</li> </ul>

- **Category 1:** These are the class of violations for which disclosure currently is required under the ITAR (*i.e.*, violations involving 22 C.F.R. §126.1 countries or nationals). There would not be any change to the existing regulatory reporting requirements as these presumably involve the highest level of threat to national security and public policy considerations.

DDTC would continue to employ their current internal processes for Category 1 violations. However, the WG suggests that DTCC could implement its own internal “triage” process to identify/focus on cases of actual concern. For example, there would appear to be a substantial difference in impact on national security between the unauthorized export of Defense Articles to a Chinese military-affiliated entity in China versus an unlicensed export of Defense Articles to a U.S. Government contractor operating in Afghanistan.

- **Category 2:** These are the class of violations that involve a loss, compromise or suspected compromise of Defense Articles (including Technical Data) or provision of a Defense Service. The expectation is that if a company<sup>9</sup> determines to disclose such a violation, it would proceed under the current VD process<sup>10</sup> and provide the necessary details, root cause analysis, and corrective action to allow regulators to assess risk, impact, and any additional actions.

The classification of a potential violation as a Category 2 violation would be a presumption. In other words, it is possible that a violation initially classified as Category 2 could be changed to a Category 3 violation based on the presence of significant mitigating factors. For example, an exporter had multiple licenses for the export of the same part number, to the same customer, for the same program in the same NATO country.

- **Category 3:** These are the class of violations that do not involve either (a) a loss or compromise of Defense Articles (including Technical Data) or (b) performance of a Defense Service. Based on the information available to the WG, these violations are unlikely to implicate national security or foreign policy considerations.

Appendix A includes a spreadsheet that identifies selected ITAR requirements and classifies a violation of each requirement as Category 1, 2, or 3 based on the methodology described above.

If a company desires to disclose Category 3 violations, the WG recommends that DDTC establish an alternative disclosure process, as discussed below. The suggested alternative process will enable DDTC to meet its requirements for receiving information on violations while providing industry flexibility in addressing “administrative” violations.

---

<sup>9</sup> The terms “Company” and “U.S. Person(s)” used throughout this white paper are used synonymously and adopt the definition of “U.S. Person” as defined by 22 C.F.R. §120.15.

<sup>10</sup> 22 C.F.R. §127.12

Like Category 2 violations, the designation of Category 3 is a presumption that can be changed (or rebutted) based on the presence of significant aggravating factors. For example, failure to maintain a copy of a shipping record for one shipment would likely be a Category 3 violation. However, an intentional decision to destroy records for all exports for a certain program because of a concern regarding the end user would be a substantial aggravating factor that could change the Category 3 violation into a Category 2 violation (and also could result in DDTC rescinding the company's ability to use the alternative processes for Category 3 violations).

#### Alternative Disclosure Process(es) for Category 3 Violations

DDTC has established precedent guidance regarding an alternative process for handling violations related to certain temporary imports of Defense Articles for repair when the U.S. importer has not correctly claimed the 22 C.F.R. §123.4(a)(1) on the customs entry documents.<sup>11</sup>

In short, instead of submitting a VD under 22 C.F.R. §127.12, a U.S. importer can review the situation and, if it determines that it was not at fault for the improper import (*e.g.*, the foreign person sent the Defense Articles without any notice), the U.S. importer can apply for a DSP-5 license to return the items and explain why it was not at fault in the Supplementary Explanation of Transaction. If DDTC agrees, it will approve the license. This process allows DDTC to receive information about a violation of ITAR requirements, but does not require a complete VD under 22 C.F.R. §127.12 to resolve the matter.

This same type of alternative disclosure process involving reporting and corrective actions should be extended to other Category 3 violations. Options for alternative processes may include the following:

- Periodic reports or “binning” of Category 3 violations
- Report Category 3 issues in applications
- Notification to DDTC of corrective action (*e.g.*, upload required document/notice with cover letter explaining issue and corrective action)

The objective is to provide alternatives to resolve Category 3 violations without filing a VD because they are “administrative” in nature and do not involve loss or compromise of controlled products or information. When this situation occurs, the U.S. person would be required to investigate the nature and cause of the violation, then, in lieu of submitting a separate VD in accordance with 22 C.F.R. §127.12, the U.S. person could provide notice or submit a report via the alternative method to notify DDTC of the error, explain the reasons why the violation occurred, and the corrective actions put in place to prevent it from occurring again.

---

<sup>11</sup> See DDTC web guidance at [http://www.pmdtc.state.gov/licensing/documents/WebNotice\\_TemporaryImportViolations.pdf](http://www.pmdtc.state.gov/licensing/documents/WebNotice_TemporaryImportViolations.pdf).

The WG proposes that DDTC implement this process to address all types of Category 3 violations (*i.e.*, “administrative violations”). Suggestions for alternative processes for the Category 3 violations are included in Appendix A. This will presumably lower the number of VDs submitted to DDTC, but at the same time, offer alternative methods of reporting.

Also, the WG notes that DDTC could rescind the use of such alternative process for any U.S. person that was found to violate a section or numerous sections of the ITAR on a repeated basis or who otherwise abuses the alternative process.

This option for an alternative to the existing VD process will provide U.S. persons with an opportunity to demonstrate an effective risk management system that highlights continuous improvement. The alternative process also provides DDTC with information needed for compliance analysts to conduct an initial review and determine if the incident poses additional concerns or if the corrective actions are adequate. U.S. persons would also identify mitigating and aggravating factors that help make the case for an isolated versus a systemic failure. This alternative process has the potential to provide DDTC with valuable metrics and at the same time allow U.S. persons the opportunity for increased partnership.

***b. Review the Department of State’s approach to regulatory enforcement versus the Department of Commerce’s approach and analyze how or if the approaches could be synchronized and/or modified;***

Based on our research and the input that the WG received, industry’s general perception of differences between the enforcement approaches of DDTC and DoC is as follows:

- DTCC: Characterized by “administrative compliance” which means that the agency’s focus is to help industry implement corrective measures to ensure compliance rather than punish previous noncompliance.
- DoC: Characterized as “law enforcement,” which means that the view is that the primary objective is to investigate and assess penalties for noncompliance, with a secondary objective of ensuring corrective actions are implemented.

Positive elements from DTCC that could be adopted by DoC include (a) establishing a process to address less serious violations administratively (*e.g.*, use of compliance analysts rather than special agents to review less sensitive violations) and (b) place a greater emphasis on corrective measures and less on assessing penalties and publicizing settlements.

Positive elements from DoC that could be adopted by DTCC include the 180-day extended timeframe for VDs. The general view in industry is that DDTC’s 60-day time frame for VDs does not allow for a sufficiently thorough review and analysis of the violations and possible corrective measures. This reality impacts DDTC in the form of repeated requests for extension that are routinely granted. Eliminating the need for such requests by allowing sufficient time to investigate and prepare VDs would conserve agency resources. It would also likely increase the quality of industry submissions.

Finally, the WG reviewed other VD process improvements that would have a positive impact on the trade compliance process at DDTC:

- Public Change in Expectations: Within industry, many companies believe that DDTC takes the position that disclosures of violations are required and are not voluntary. This has developed because of past statements by DDTC in conferences and forums where companies are advised to disclose violations, and comments that lack of VDs is a sign that company's compliance program is not functioning correctly. To reduce VDs involving "administrative" violations, DDTC could modify how it publicly speaks about the VD process and recognize that industry has discretion to not submit disclosures for violations other than those involving 22 C.F.R. §126.1 countries or nationals.
- Case Officer Assignment Process: The WG believes that both DTCC and industry would benefit if disclosures from the same company or USML Category were assigned to the same case officer or officers. This would allow the case officer(s) to develop the expertise and background to assess disclosures from a particular company or related to a particular type of product. In addition, it would facilitate understanding of expectations and requirements for both DTCC and industry.
- Increase Interagency Coordination for "Transition" VDs: The WG recommends that DTCC and DoC develop a process to either assign a lead agency for multi-agency matters or establish a process where a company only needs to prepared and submit one VD for underlying conduct and then provide copies of the disclosure to all other agencies that may be implicated.

*c. Consider whether VD policies or procedures from other regulatory agencies may have elements that could be of benefit for State; and*

The WG researched regulations and policies of other U.S. Government agencies related to VDs to identify positive elements that may warrant consideration by DDTC. Details from the WG research are provided in Appendix B. The four main elements identified by the WG were as follows:

- Electronic Submission Process
  - Customs and Border Protection (CBP), Environmental Protection Agency (EPA), Department of Health and Human Services (HHS), Department of the Treasury (Treasury)
- Administrative "Binning" Process
  - CBP and Census Bureau (Census)

- Clear benefits offered to those who disclose
  - CBP, Census, Internal Revenue Service (IRS), Nuclear Regulatory Commission (NRC), Office of Foreign Assets Control (OFAC)
- Published Guidance
  - CBP, Census, NRC, Federal Aviation Administration (FAA), Transportation Security Administration (TSA)

The consensus of the WG was that an electronic system for submission of VDs would be of greatest benefit. The system currently used for submission of information to the Committee on Foreign Investment in the United States (CFIUS) was proposed as a model as it does not require the development or use of any specific forms. Rather, it is simply an electronic system that allows U.S. parties to email documents in PDF<sup>12</sup> to a specific email address at Treasury. The email is forwarded to the relevant analyst who then responds in the same manner. It was also proposed that DDTC’s current Electronic Forms Submission (EFS) system – which allows for the submission of PDF documents directly to DDTC – could be effectively utilized for the submission of VDs.

An electronic submission system would expedite the process of obtaining a case number and analyst – which would allow companies to submit applications related to the disclosure quickly. It would also provide a system for electronic recordkeeping, and ideally process tracking, that could reduce the number of instances of lost or misplaced VDs and decrease the labor intensive process of logging and copying submissions.

***d. Review how the trade compliance process may need to change if/when State and Commerce’s trade regulatory bodies merge in the future.***

As enforcement efforts increase and the cooperation among the various government agencies also increases, the need for a multi-agency disclosure process is crucial for industry compliance programs with limited budgets and personnel resources. The WG encourages changes to the VD process to increase national security focus by facilitating greater partnership with industry in order to effectively manage risk.

---

<sup>12</sup> “PDF” is an acronym referring to the portable document format.

## Summary and Conclusion

- Proposed methodology for identifying Category 3 (*i.e.*, “administrative”) violations
  - No change to current requirements for 22 C.F.R. §126.1 matters
  - Based on “loss or compromise” standard; *and*
  - Analysis of aggravating/mitigating factors
- Suggested alternatives to 22 C.F.R. §127.12 process for Category 3 violations
  - *See* Appendix A for categorization of selected ITAR provisions and suggested alternative processes
- Additional process changes
  - DTCC to modify public statements regarding expectations for VDs
  - Modify case officer assignment process
  - Implement electronic submission process

## Appendices

- A. Chart of Presumptive Category for Violations for Selected ITAR Requirements
- B. Summary of Research into Voluntary Disclosure Program of Other USG Agencies

**Appendix A: Chart Showing Presumptive Category for  
Violation of Selected ITAR Requirements**

ITAR Section	Violation Category	Option(s) for Alternative Process (Category 3)
<b>Part 122 - REGISTRATION OF MANUFACTURERS AND EXPORTERS</b>		
§122.1 - Requirement to register if engaged in the U.S. in the business of manufacturing, exporting or temporarily importing defense articles or furnishing defense services	3	Submit registration and notify DDTC that you should have registered at an early date. Include root cause and corrective action(s)
§122.4(a) - Five-day notification requirement for specified changes in information contained in registration statement	3	Submit notice with explanation of why notice was not timely, root cause and corrective action(s)
§122.4(b) - 60-day advance notification requirement for intended sale or transfer to a foreign person of ownership or control of the registrant	3	Submit notice with explanation of why notice was not timely, root cause and corrective action(s)
§122.4(c) - Notification requirement when registrant merges with another company or acquires, or is acquired by, another company	3	Submit notice with explanation of why notice was not timely, root cause and corrective action(s)
§122.5 - Five-year recordkeeping requirement for registrants	3	Submit a notice that recordkeeping issues identified and describe corrective action(s)
<b>Part 123 - LICENSES FOR THE EXPORT AND TEMPORARY IMPORT OF DEFENSE ARTICLES</b>		
§123.1(a) - License requirement for export or temporary import of defense articles	2	
§123.3(a) - License (DSP-61) requirement for temporary import and subsequent export of unclassified defense articles	3 <i>(for import &amp; return)</i>	Apply for DSP-5 to return and provide explanation in application, along with root cause and corrective action(s)
	2 <i>(for trans-shipment)</i>	
§123.4 - Exemptions for temporary import (and subsequent export) of unclassified U.S.-origin defense articles	3	Alternative process already in place <i>(Temporary Import Violations)</i>
§123.5 - License (DSP-73) requirement for temporary export and subsequent return of unclassified defense article	2	
§123.8 - License requirement for transfer of registration/control of vessels, aircraft and satellites covered by the USML to foreign person or registration of vessel, aircraft or control in foreign country	2	
§123.9(a) - Requirement to obtain DDTC approval prior to reselling, transferring, transshipping, or disposing of a defense article to any end user, end use or destination other than as stated on the export license or EEI (for exemptions)	2	

§123.9(b) - Requirement to include destination control statement on bill of lading, airway bill or other shipping document and on purchase documentation or invoice	3	Notify recipients of jurisdiction/classification of items & retain documentation
§123.9(e) - Reexports or retransfers of U.S.- origin components incorporated into a foreign defense article to NATO, NATO agencies, a government of a NATO country, or the governments of Australia, Israel, Japan, New Zealand, or the Republic of Korea	2	
§123.10 - Requirement to provide signed DSP-83 for export of SME or classified defense articles	3	
§123.11(a) - Requirement for a license when a privately owned aircraft or vessel on the USML makes a voyage outside the United States	2	
§123.13 - Requirements applicable to domestic aircraft shipments via a foreign country	2	
§123.16 - Exemptions for exports of unclassified defense articles under various circumstances	2	
§123.17 & .18 - Requirements for exports of firearms, ammunition, and personal protective gear	2	
§123.22 - Requirements for license presentation/lodging/return, submission of EEI via AES for all exports of defense articles and reports of various types of technical data/defense service exports	3	Census and/or CBP disclosure, then provide notice of disclosure to DDTC. Include root cause and corrective action for violation
§123.26 - Recordkeeping requirement for exemptions	3	Submit a notice that recordkeeping issues identified and describe corrective action(s)
<b>Part 124 - AGREEMENTS, OFF-SHORE PROCUREMENT AND OTHER DEFENSE SERVICES</b>		
§124.1(a) - Requirement to obtain DDTC approval to provide defense services to foreign persons	2	
§124.1(c) - Requirement to obtain DDTC approval for any amendments that change the scope of approved Agreements	2	
§124.2 - Exemptions for training and military service	2	
§124.4(a) - Applicant must file a copy of the concluded TAA or MLA with DDTC not later than 30 days after Agreement enters into force	3	Upload executed agreement to D-Trade with cover letter that explains reason for missed deadline, root cause & corrective action(s)
§124.4(b) - Application must furnish additional information specified in paragraphs (1) - (4) when submitting executed copy of MLA	3	Upload letter with required information to D-Trade - Include reason for missed deadline, root cause & corrective action(s)

§124.5 - Applicant must inform DDTC if a decision is made not to conclude an approved agreement within 60 days of the decision	3	Upload notice with required information to D-Trade - Include reason for missed deadline, root cause & corrective action(s)
§124.6 - Applicant must inform DDTC in writing of impending termination of Agreement not less than 30 days prior to expiration date	3	Upload notice with required information to D-Trade - Include reason for missed deadline, root cause & corrective action(s)
§124.16 - Retransfer authorization for unclassified technical data and defense services to member states of NATO and EU, Australia, Japan, New Zealand & Switzerland	2	
<b>Part 125 - LICENSES FOR THE EXPORT OF TECHNICAL DATA AND CLASSIFIED DEFENSE ARTICLES</b>		
§125.1(b) - Requirement to obtain DDTC approval to use a license for the export of technical data or §125.4 exemptions for technical assistance or foreign production purposes	2	
§125.1(c) - Requirement to obtain DDTC approval for the reexport, transfer or diversion of technical data from country of ultimate end-use or authorized foreign end-user	2	
§125.2(a) - License requirement for the export of unclassified technical data	2	
§125.2(b) - License requirement for export of technical data in connection with foreign filing of patent applications	2	
§125.2(c) - License requirement for the oral, visual or documentary disclosure of technical data by U.S. persons to foreign persons	2	
§125.3 - License requirement for the export of defense articles (including technical data) that have been classified by the U.S. or a foreign government	2	
§125.4(a) - Exemptions for the export of technical data	2	
§125.6(a) - Requirement to certify that a proposed export is covered by a relevant exemption at the time of export	3	
§125.6(b) - Requirement to complete and retain a written certification that a proposed oral, visual or electronic export is covered by a relevant exemption	3	Create record(s) with explanation of basis for determination and reason why not created at time of activity
<b>Part 126 - GENERAL POLICIES AND PROVISIONS</b>		
§126.1(b) - Prohibition on the export, temporary export, retransfer or reexport of defense articles on a vessel, aircraft, spacecraft or conveyance owned by, operated by, leased to or leased from any proscribed country	1	
§126.1(c) - Prohibition on transactions subject to the ITAR involving a country when U.S. Security Council mandates an arms embargo on that country	1	

§126.1(e)(1) - Requirement to obtain a license for the sale, export, transfer, reexport, or retransfer of defense articles to proscribed countries	1	
§126.1(e)(1) - Requirement to obtain a license to make a proposal or presentation to export, transfer, reexport, or retransfer defense articles to proscribed countries	1	
§126.1(e)(2) - Requirement to notify DDTC immediately if knowledge or reason to know of proposed, final or actual sale, export, transfer, reexport, or retransfer of defense articles or defense services to proscribed countries	1	
§126.4 - Exemption for shipments by or for U.S. Government agencies	3	Submit notice to DTCL that exemption used and explain reason(s) for noncompliance
§126.5(a) - Exemption for the temporary import of defense articles from Canada for use in the United States and return to Canada	3	
§126.5(b) - Exemption for the temporary and permanent export of defense articles to Canada for end use in Canada or return to the United States	2	
§126.5(d) - Requirement for DDTC approval for the reexport/retransfer to another end user or end use in Canada or from Canada to a destination other than the United States	2	
§126.16 - Exemptions pursuant to the Defense Trade Cooperation Treaty between the United States and Australia	2	
§126.17 - Exemptions pursuant to the Defense Trade Cooperation Treaty between the United States and the United Kingdom	2	
§126.18 - Exemptions regarding intra-company, intra-organization, and intra-governmental transfers to employees who are dual nationals or third-country nationals	2	
<b>Part 129 - REGISTRATION AND LICENSING OF BROKERS</b>		
§129.1 - Requirement to provide annual report of brokering activities with registration renewal	3	Alternate process already in place (Hold processing until report provided)
§129.4 - Requirement to obtain prior approval for brokering activities involving defense articles or defense services listed in (a)(1) or (a)(2)	2	
§129.7(b) - Requirement for DDTC approval to engage in or make a proposal to engage in brokering activities with a proscribed country, area or person	1	
§129.7(c) - Requirement for DDTC approval to engage in or make a proposal to engage in brokering activities that involve countries or persons subject to restrictions imposed by the USG for reasons of national security, foreign policy or law enforcement	1	

§129.8(b)(2) - Requirement to submit brokering registration at least 30 days prior to expiration date	3	Submit renewal with explanation of why not timely, including root cause & corrective action(s)
§129.8(d) - 5-day notification requirement for changes in registration statement set forth in §129.8(d)(1) or (d)(2)	3	Submit notice with explanation of why it was not timely, including root cause & corrective action(s)
§129.8(e) - 60-day notification requirement for intended sale or transfer to a foreign person of ownership or control of the registrant or any affiliate	3	Submit notice with explanation of why it was not timely, including root cause & corrective action(s)
§129.11 - Recordkeeping requirement for registered brokers	3	Submit a notice that recordkeeping issues identified and describe corrective action(s)
<b>Part 130 - POLITICAL CONTRIBUTIONS, FEES AND COMMISSIONS</b>		
§130.9(a) - Requirement for applicant to furnish information on payment (or agreement to pay) political contributions or fees and commissions above specified thresholds in connection with transaction for which authorization is being requested	3	Include notice of omission when reporting and describe root cause & corrective action(s)
§130.9(a) - Requirement for supplier to furnish information on payment (or agreement to pay) political contributions or fees and commissions above specified thresholds	3	Include notice of omission when reporting and describe root cause & corrective action(s)
§130.9(d) - Requirement for applicant or supplier to furnish updated information within 30 days	3	Include notice of omission when reporting and describe root cause & corrective action(s)
§130.11 - Requirement for applicant or supplier to submit supplementary reports	3	Include notice of omission of supplementary reports when reporting, include root cause & corrective action
§130.12 - Requirement of applicant and supplier to obtain information on political contributions and fees or commissions from each vendor	3	Report required information, include in submission explanation of why not previously included, root cause & corrective action
§130.14 - Requirement for each applicant, supplier and vendor to maintain records for a period of not less than five years following the date of the report to which they pertain	3	Submit a notice that recordkeeping issues identified and describe corrective action(s)

## Appendix B: Research on Voluntary Disclosure Program of Other USG Agencies

Reviewed:

- Customs – Prior Self-Disclosures
- OFAC – “Informal” Voluntary Disclosure process
- IRS – Voluntary Disclosure
- Census’ Foreign Trade Regulations – Voluntary Self-Disclosure
- NRC – No formal VD process, but “credit” for self-identification of violations
- Department of Defense – Voluntary Disclosure
- EPA – “Voluntary Self-Disclosure”
- FAA – “Voluntary Disclosure”
- HHS – “Contractor Self-Disclosure”
- Federal Acquisition Regulations – Mandatory Disclosure Rule

Details:

US Government Agency	Positive Elements
<b>Bureau of Industry and Security (BIS)</b>	<ul style="list-style-type: none"> <li>• CCL Part 764.1 provides detailed information association with violations</li> <li>• Supplement No. 1 to Part 766 ; describes how BIS responds to violations and how it typically exercised its discretion regarding whether to pursue an administrative enforcement</li> <li>• Violations are to be disclosed “as soon as possible”</li> <li>• The initial notification date is the date received by the Office of Export Enforcement</li> <li>• Option to disclose a violation orally, with a confirmation in writing as soon as possible</li> <li>• Final Due 180 days of the initial notification; long lead time</li> <li>• Oral presentations can be requested</li> <li>• BIS Warning and “Closure No Action” Letters at times may come with an offer by BIS to conduct outreach training</li> <li>• Anti-boycott Issues/Concerns; industry is allowed to call and request advice</li> </ul>
<b>Census Bureau</b> <ul style="list-style-type: none"> <li>• Disclosure of violations of the FTR.</li> </ul>	<ul style="list-style-type: none"> <li>• Guidance outlined in Foreign Trade Regulations, 15 CFR Part 30.74</li> <li>• Provides sample guidance on website</li> <li>• Allows you to combine multiple transactions in one disclosure</li> <li>• Recommends review/disclosure back five years</li> </ul>
<b>Customs and Border Protection (CBP)</b> <ul style="list-style-type: none"> <li>• Disclosure of Import Violations of 19 USC 1592</li> </ul>	<ul style="list-style-type: none"> <li>• Recognized prior disclosure process with published guidance</li> <li>• Mitigation of civil penalties</li> <li>• Other published mechanisms for reporting and correcting administrative errors, although they do not provide mitigation of civil penalties.                             <ul style="list-style-type: none"> <li>• Post Entry Amendment (PEA) process – correction of entry mistakes prior to liquidation.                                     <ul style="list-style-type: none"> <li>• “Binning” and quarterly reporting of errors with a Customs duty impact &lt;\$20 (owed or refund)</li> </ul> </li> <li>• Protest process – allows for recovery of overpayment of Customs duties up to 90 days after liquidation.</li> <li>• Voluntary Tender – allows for payment of Customs duties owed.</li> </ul> </li> </ul>

US Government Agency	Positive Elements
<b>Customs and Border Protection (CBP)</b> <ul style="list-style-type: none"> <li>Disclosure of a violation of the Foreign Trade Regulations (FTR) (Export)</li> </ul>	<ul style="list-style-type: none"> <li>Drafted guidelines with a review of DHS and DOC</li> <li>Separates mitigation schemes (each one with a separate criteria) <ul style="list-style-type: none"> <li>I. The failure to file the export information in AES</li> <li>II. The late filing of the export information in AES</li> <li>III. The failure to file all the necessary information in AES, the filing of incorrect information in AES, or failure to comply with some other requirement of the FTR</li> <li>IV. The failure of the exporting carrier to provide certain documents or certain information to CBP</li> </ul> </li> <li>Offers special handling of certain circumstances</li> <li>Penalties can be applied to all parties involved not just the one disclosing</li> <li>Penalties are assessed per each AES transaction rather than per violation</li> <li>The decision whether or not to impose penalties heavily weighs on “informed compliance” (i.e. first time offenses, alternative to educate and inform industry, company outreach, etc.</li> </ul>
<b>Environmental Protection Agency (EPA)</b>	<ul style="list-style-type: none"> <li>Electronic Submittal Available</li> <li>Provides annual results of enforcement accomplishments; including those not penalized however showing a significant compliance program put in place</li> </ul>
<b>Internal Revenue Service</b>	<ul style="list-style-type: none"> <li>Mitigating factor used by IRS in determining whether criminal prosecution will be recommended.</li> </ul>
<b>Office of Foreign Assets Control (OFAC)</b>	<ul style="list-style-type: none"> <li>Offers penalty mitigation of 50% of base penalty, when self-disclosed.</li> </ul>

US Government Agency	Positive Elements
<b>Federal Aviation Administration (FAA)</b>	<ul style="list-style-type: none"> <li>Issues Guidance on the five types of actions related to FAA enforcement <ul style="list-style-type: none"> <li>I. Administrative Action <ul style="list-style-type: none"> <li>FAA considers a violation minor if the action was not deliberate, was not significantly unsafe, and did not evidence a lack of competency or qualification . Warning Letter or Letter of Correction is issued</li> </ul> </li> <li>II. Re-examination Action <ul style="list-style-type: none"> <li>Can reexamine an airman at any time if the FAA has reasonable grounds</li> </ul> </li> <li>III. Certification Action <ul style="list-style-type: none"> <li>Seeks to suspend or revoke a pilots license when a violation indicates a lack of technical proficiency or qualification</li> </ul> </li> <li>IV. Civil Penalty <ul style="list-style-type: none"> <li>Used as an option only</li> </ul> </li> <li>V. Criminal Action <ul style="list-style-type: none"> <li>Applied to acts such as aircraft privacy, forgery of certificates, carry weapons aboard aircraft, etc.</li> </ul> </li> </ul> </li> </ul>
<b>Nuclear Regulatory Commission (NRC)</b>	<ul style="list-style-type: none"> <li>Strong emphasis on self-identification of violations, through self disclosure.</li> <li>Will consider providing “credit” for corrective actions and self-identification of violations.</li> <li>Fairly comprehensive guidance published in the NRC Enforcement Policy – <ul style="list-style-type: none"> <li>Identifies Severity Levels (I to IV) (highest to lowest)</li> <li>Provides good information about disposition of violations.</li> </ul> </li> </ul>
<b>Transportation Security Administration (TSA)</b>	<ul style="list-style-type: none"> <li>Published Voluntary Disclosure Program Policy</li> <li>Applies to aircraft operators (except individuals), indirect air carriers, foreign air carriers, airports and flight training providers. <ul style="list-style-type: none"> <li>They stress that the Voluntary Disclosure Program does not cover individuals.</li> </ul> </li> <li>Will issue a letter of correction in lieu of civil penalty. Case considered closed upon issuance.</li> </ul>

	OFAC	IRS	Census/FTR	NRC
Required by law or voluntary?	Voluntary	Voluntary	Voluntary	Voluntary
Benefits of Disclosing	Penalty Mitigation – 50% of base penalty	Mitigating factor used by IRS in determining whether criminal prosecution will be recommended	Mitigating factor used by Census in determining what administrative sanctions, if any, will be sought.	If problem requiring corrective action was self-identified and corrective action is promptly taken, no civil penalty.
Timing of Disclosure	Prior to or at the same time USG discovers the apparent violation or another substantially similar	Prior to the IRS initiating a civil exemption, regardless of whether I relates to undisclosed foreign accounts or undisclosed foreign entities, the taxpayer will not be eligible to come in under the IRS's Voluntary Disclosure Practice	Prior to Census or any other USG agency learning the same or substantially similar information from another source, and the commencement of an investigation or inquiry in connection with that information.	Prior to discovery by USG

#### U.S. Customs & Border Protection – Prior Disclosures, Post Entry Amendments & Protests

	Prior Disclosure (PD)	Post Entry Amendment (PEA)	Protest	Voluntary Tender
Required by law or voluntary?	Voluntary	Voluntary	Voluntary	Voluntary
When must it be filed?	Prior to CBP discovery	Prior to Liquidation	After Liquidation	Prior to CBP discovery
Offers relief from penalties?	Yes	No	No	No
What is it used for?	Reporting a violation of 19 U.S.C. 1592	Correction of an entry mistake	Refund of Customs Duties	Payment of Customs Duties
How is it filed?	Letter, to local CBP office	Letter, to local CBP office or via ACE	CF19 form, to local CBP office	
Offers special handling of certain circumstances?	No	Yes: Administrative corrections may be “batched” in quarterly reports, when the Customs duty impact is <\$20 per entry (owed or refund)	Yes: you may request further review by someone other than the local port.	No