Defense Trade Compliance

Marissa Cloutier
Defense Trade Controls Compliance

May 2016
Overview

- Why Compliance?
  - AECA/ITAR
  - National security
- Case Studies
- Voluntary/Directed Disclosures
  - Observed violations
  - Submitting disclosures
- Compliance Program Elements
Why does compliance matter?

• It’s the law
  – U.S. and foreign individuals and entities are liable
  – Fines, penalties, and possible jail time for violations of the ITAR

• Supports national security and foreign policy initiatives
  – Unauthorized transfers may harm U.S. national security and foreign policy interests

• Compliance is good for you
  • Affects your organization’s reputation
  • Enables you to keep reaching for your organization’s objectives
  • Avoids costs needed to address non-compliance

Export control laws are meant to protect U.S. national security by controlling the release of U.S.-origin technology

The U.S. government determines whether the release of certain technology will support or harm our national security
Governing Statute and Regulations

- **Arms Export Control Act (AECA) (22 U.S.C. 2778-2780)**
  - Law governing defense trade
  - Section 38 authorizes the President to control the export and import of defense articles and defense services and to designate those items
  - The AECA generally requires a license as a condition of exporting or importing defense articles and defense services

- **International Traffic in Arms Regulations (ITAR) (22 CFR 120-130)**
  - Federal regulations that implement the Arms Export Control Act
  - Establish the policy, licensing and compliance framework for the trade control function administered by the Departments of State and Defense
  - Detail the U.S. Munitions List (USML)
Penalties & Procedures

• Penalties associated with AECA/ITAR violations:
  • Costs associated with review; resolution of issues
  • Denial or revocation of export authorizations
  • Administrative penalties under ITAR § 128
    • Generally settled through a negotiated Consent Agreement

What is a Consent Agreement?
• Agreement that includes a monetary penalty and enforceable conditions, such as:
  • Review, audit, and reporting requirements
  • Compliance program improvements
  • Debarment, if applicable
  • Appointment of a Special Compliance Official
• Typically run 3-4 years
• Monitoring by DTCC
National Security

• Proposed transfers of defense articles, including technical data and defense services are assessed by DOD for national security implications

• U.S. government has the technological know-how and resources (review by appropriate agencies) to perform assessments and make determinations

• Factors considered
  – Foreign policy (region, country)
  – Level of technology
  – End user and end use
  – Military operational impact
  – Inter-operability requirements
  – Bilateral, multilateral and international agreements
  – Foreign availability of like systems
  – Classified data transfers
Case Study

• 2015: University A1 pursues external funding for the development of robotic arm. University performs self-classification and determines research is not ITAR-controlled. University A1 accepts funding, and work (including by foreign person, as defined in the ITAR) begins on the project. Three months into the project a research partner informs University A1 that the project is ITAR-controlled; University A1 disagrees. University A1 may have committed a violation.

Suggested next steps:

– Stop foreign person’s access to the technology
– Review self-classification decision
– If in doubt request a Commodity Jurisdiction determination (ITAR 120.4)
– Submit voluntary disclosure to the Office of Defense Trade Controls Compliance if possible violation occurred (ITAR 127.12)
Case Study

• 2015: A company exports an ITAR-controlled item in 2011 without authorization. As a result of the Export Control Reform the item transitioned to the Department of Commerce on October 15, 2013, and is now EAR-controlled.
  – Should you disclose this violation?
    • Yes—the violation should be reported
  – Which USG agency gets the disclosure?
    • Although the item may no longer require authorization from the Department of State, the violation occurred while the item was under DOS jurisdiction – so disclose to State
  – What do you do if you want to change the end-use/end-user after the item transitioned? Request authorization from Commerce

Consult DDTC for authoritative guidance
Observed Violations

- Incorrect jurisdiction and downstream effects
- Failure to register
- Unauthorized access to defense articles and technical data
- Misuse of ITAR exemptions
- Failure to mark documents
- Misunderstanding or misuse of definitions and downstream effect (i.e., fundamental research)
- Failure to maintain records
- Unauthorized exports
- Involvement of 126.1 countries and unauthorized foreign nationals
# Disclosures

**Voluntary Disclosure (VD)**

Persons voluntarily disclose circumstances to DTCC which they believe may have violated any export control provision of the AECA, or any regulation, order, license or other authorization issued

**Directed Disclosure (DD)**

In the form of a letter, DTCC requests information regarding a potential or actual violation, based on other information received from other sources

Information sources: calls, emails, inter-agency, intra-agency, other disclosures

<table>
<thead>
<tr>
<th>ITAR § 127.12</th>
<th>Based on ITAR § 122.5(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,055 voluntary disclosures in FY 2015</td>
<td>56 directed disclosures in FY 2015</td>
</tr>
</tbody>
</table>

NOTE: Failure to report will be a factor in determining any penalties
Voluntary Disclosure Notification

• Provide initial notification immediately after a violation is discovered, then a full disclosure after thorough review
  • 60 day period to submit, per ITAR § 127.12(c)(1)(i)
  OR

• Provide full disclosure immediately after a violation is discovered

Full disclosure should include all information identified in ITAR § 127.12(c)(2)
Compliance Program

Elements

• Senior officer’s **commitment** to compliance

• A **knowledgeable** Empowered Official

• Established **protocols** and **procedures**

• Adequate **resources** dedicated to compliance

The best compliance programs are tailored to your organization and its operations. They don’t need to be complicated – they need to work. For general guidelines, see: [http://www.pmddtc.state.gov/compliance/documents/compliance_programs.pdf](http://www.pmddtc.state.gov/compliance/documents/compliance_programs.pdf).
Questions and Guidance

• General Questions – DDTC Response Team
  Phone number: (202) 663-1282
  E-mail: DDTCResponseTeam@state.gov

• For specific questions, visit website
  https://www.pmdddtc.state.gov/ECR/index.html