United States Department of State
Bureau of Political-Military Affairs
Office of Defense Trade Controls Compliance
Washington, D.C. 20520-0112

DTCC Company Visit Program: Summary Report 1
May 2015 through April 2016

DTCC relaunched its company visit program (“CVP”) in 2015. The program includes onsite visits to industry as an extension of DDTC’s outreach initiatives (“CVP-O”) and engagement in existing compliance cases (“CVP-C”). CVP creates value through increased face-to-face interactions with industry, and benefits the entire Directorate by creating opportunities to share information internally and externally. This report is part of the program relaunch; additional reports summarizing CVP activity will follow. The reports will share some company best practices, provide recommendations for improving compliance programs, and include firsthand information we learned through our onsite interaction. The information included in this report is limited to our site visits and does not include observations or recommendations identified through disclosures or other enforcement activities. The reports are non-attributional and do not include any data identified as being related to a specific company.

Summary of Visits
May 2015 – April 2016

Start Date	End Date	Visit Type	Location
5/1/15	5/1/15	CVP-C Consent Agreement (CA) Monitoring	Poland
6/15/15	6/15/15	CVP-C CA Monitoring	GA
8/20/15	8/21/15	CVP-O	CO
8/18/15	8/19/15	CVP-C Reinstatement	CO
9/28/15	9/30/15	CVP-C CA Monitoring	Canada
11/16/15	11/16/15	CVP-O	VA
12/7/15	12/8/15	CVP-O	MA
12/10/15	12/11/15	CVP-O	RI
12/21/15	12/27/16	CVP-C CA Monitoring	WA & CA
3/9/16	3/10/16	CVP-O	UAE

Start Date	End Date	Visit Type	Location
3/9/16	3/10/16	CVP-O	UAE
2/8/16	2/13/16	CVP-C CA Monitoring	CA & AZ
4/11/16	4/15/16	CVP-C CA Monitoring	CA
4/21/16	4/21/16	CVP-O	Belgium
4/22/16	4/22/16	CVP-C CA Monitoring	Belgium

Best Practices Noted During Visits:

- Requiring suppliers to complete a standardized form identifying the jurisdiction/classification of their products and related technical data. Use of such a form may drive more companies to take an active role in identifying and documenting the export control jurisdiction of their products. The form also serves as a standardized tool for clear and consistent recordkeeping.

- Integrating export control processes into company quality systems and reviews.

- Physically segregating ITAR-controlled research (including research using ITAR-controlled articles or technical data) at universities.

- Providing foreign customers with a summary of TAA requirements, and tying those requirements to the contract with the foreign end-user. This may help expedite the TAA signature process, and can serve as a tool to educate the foreign customer on limitations that may exist when procuring U.S. services and technical data.

- Incorporating export compliance reviews into IT systems that manage project lifecycles, so that the workflow requires approval from the export compliance function prior to the bid/no-bid business decision.

- Requiring self-classifications to be reviewed and signed by engineering and technology managers of the cognizant business *and* a senior technology manager from a separate business unit, serving as an independent peer reviewer.

- Using incentive programs, such as internal recognition and/or awards, to recognize employees for compliance activities.

Recommendations/Observations for Improvement:

- U.S. companies may consider additional outreach and training on ITAR compliance for foreign partners and customers.

- Processes for identifying dual and third country nationals (DTCNs) should include a requirement to review the bona fide regular employee status in accordance with ITAR Section 126.18.

- A U.S. applicant should consider including in contracts with foreign parties terms and conditions that ensure it has direct physical access to its U.S. person employees providing defense services. This allows the U.S. applicant to directly oversee compliance of its employees, as required per ITAR 127.1(c).

- In order to maintain objectivity, universities should ensure internal, independent reviews are used to determine the ITAR-controlled status of current programs and future opportunities.

- Compliance personnel should identify and document all IT systems that store, or have the potential to store, ITAR-controlled technical data. A current record of who has access to these applications should be maintained.

DTCC Takeaways

- With growing frequency, U.S. persons are employed abroad to assist with maintenance, operation and training related to U.S. defense articles acquired by foreign military forces. These activities by U.S. persons may constitute defense services, requiring DDTC registration and authorization coverage. DTCC also notes that former U.S. military personnel who will be working for foreign government-owned entities while carrying out such activities may not be aware – and their would-be employers may not be aware – of separate DOD employment authorization requirements applicable to these arrangements.

- DDTC should consider increasing its outreach and training initiatives for foreign parties to ITAR authorizations.

- Companies continue to invest in the areas of IT security and data protection. DDTC should consider providing guidance specifying when a company would be expected to maintain access logs that can verify “potential” versus “actual” access to technical data.