Risks in the common practice of sending technical data outside the U.S. -- New Jersey company penalized $400,000

Eric McClafferty

September 19, 2017

Does your company source components or parts outside the U.S.? When doing so, you need to be careful about sending unlicensed export controlled technical data like drawings, blueprints and manufacturing instructions as part of an RFQ or production process. Many companies send such information to overseas parts vendors and to non-U.S. person employees at domestic vendors without a systematic check to see if the information requires an export license. And an increasing number of companies already have -- or are establishing -- offshore engineering centers of their own, or they have a relationship with an offshore third party engineering center, without focusing on the need to implement a rigorous process to ensure that data exchanged with those centers is licensed for export when needed. Similar challenges arise when engineers and procurement personnel at U.S.-based business units collaborate with a sister facility abroad, or they use web-based collaborative platforms (e.g. Sharepoint) for product development without thinking through export control concerns.

Yes, technical data export issues are more difficult to address in the same systematic way that product export issues are handled. Decision making about what data is shared and how it is shared (email, express mail, uploading to a vendor's website, data sharing sites, cloud-based platforms, etc.) is often up to individual engineering and procurement personnel. Because human beings are involved, export control training on technical data issues is key, as is implementing a fail-safe process to classify and control data. Many companies are still guessing about data classification, getting it half right, or otherwise don't have a good handle on what kind of information they are exporting. But data classification and data handling can be tamed in a way that works within your company's existing business systems. You don't need an expensive technical solution.

A case in point: A New Jersey-based manufacturer of military spare parts recently settled a voluntary self-disclosure case with the State Department for $400,000. That case involved 11 alleged violations of the International Traffic in Arms Regulations (ITAR) related to exports of technical data. Allegedly, a senior employee and people under his supervision would 'cut and paste' information from export-controlled drawings and use the relabeled drawing to obtain quotes from overseas vendors, often without export licenses. This practice apparently occurred at a company that had obtained over 500 DDTC licenses in the last 8 years, demonstrating that even companies with significant experience with ITAR and EAR licensing can have issues with technical data exports.

In fact, too many companies are turning a blind eye to weak technical data export control systems and it could catch up with them in a variety of ways, such as a whistleblowing disgruntled employee,

a competitor’s complaints, a customer’s questions about where parts and components are sourced, Buy America and Berry Amendment compliance audits and reviews, and internal financial and compliance audit processes. This is a tricky issue, but it can be addressed in a way that lets you sleep at night!