MILLER CANFIELD

Is Your Software a Defense Article?

January 14, 2015

[This article was originally published in the January 2015 issue of National Defense*, the National Defense Industrial Association's business and technology magazine, under the title, "Know When Software Falls Under Export Control Regime".]*

The International Traffic in Arms Regulations, or ITAR, control the export of software classified as a "defense article."

The United States Munitions List [USML] contains items regulated by the ITAR, including a range of products from tanks to fighter aircraft.

However, defense articles also include items like complex military cryptographic software and rudimentary diagnostic software designed to assist in the repair of other defense articles.

In collaboratively developing or licensing software, a company may violate the ITAR by improperly disclosing or transferring software as an unauthorized export. The risks of infringing ITAR include civil fines of up to $500,000 per violation, as well as suspension or debarment from government contracts, seizure and forfeiture of the defense article, and revocation of export privileges, while potential criminal liability may include fines up to $1 million per violation and 10 years imprisonment.

An ITAR violation for improperly exporting controlled software may occur by disclosing or otherwise transferring controlled software to a foreign person, whether in the United States or abroad, or a foreign government.

Software exports may include the disclosure of source code to a foreign person through both oral and written means. Moreover, an ITAR violation may occur by using the software to perform a defense service for a foreign person. A defense service is defined broadly enough to include everything from the design and development at the beginning of a defense article's life cycle, to normal repair and maintenance during an item's life cycle, from managing the end of the article's life cycle through the actual demilitarization or destruction of the item.

The first step to determining whether software is a defense article is to understand how ITAR applies to software. The regulations apply to both software specifically listed on the USML, such as military cryptographic software, and software not specifically listed on the munitions list, but otherwise classified as ITAR technical data.

The ITAR definition of a defense article includes any item or technical data designated on the munitions list, defined to include "information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles, as well as software directly related to defense articles."

Software, as defined by ITAR includes, "system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis and repair."

Software used for security, assurance systems or cryptographic devices with the following capabilities is controlled

under the ITAR because it is listed as a defense article under USML category XIII (materials and miscellaneous articles):
• Software capable of maintaining secrecy or confidentiality of information or information systems, including equipment or software for tracking, telemetry and control encryption and decryption;
• Software capable of generating spreading or hopping codes for spread spectrum systems or equipment;
• Software authorized to control access to or transfer data between different security domains as listed on the Unified Cross Domain Management Office Control List;
• Software comprising cryptanalytic systems.

Software with cryptographic functionality described in munitions list category XIII but used in ground control stations for telemetry, tracking and control of spacecraft or satellites is also controlled as a defense article in category XV (spacecraft systems and associated equipment).

Additionally, software and associated databases used to model or simulate military items tend to be controlled by ITAR because they are listed as defense articles. This type of software would be listed on category IX for military training equipment and includes: military device training software for ground, surface, submersible, space or towed airborne targets; battle management simulation software; military test scenarios and modeling software; and software that simulates the effects of weapons listed as a defense article in any munitions list category.

The inclusion of software within the definition of technical data as software directly related to defense articles broadens the potential for ITAR to control software beyond software specifically listed on the munitions list.

This broad definition of software controlled as technical data includes everything from system functional design ensuring the independence of each software module to application programs directly related to defense articles. Applying this definition of technical data to software may effectively extend ITAR controls over software by reason of merely being a support item for any defense article listed on the munitions list.

This may include everything from testing software for infantry fighting vehicles in USML category VII (ground vehicles) to operational software for controlled bombers in category VIII (aircraft), from application programs used for submarines in category XX (submersible vessels) to diagnosis and repair software for turbofan and turbojet engines in category XIX (gas turbine engines).

Regardless of whether ITAR controls the software export because such software is specifically listed on the USML or otherwise classified as technical data, an export license must be obtained, or an ITAR exemption must be applicable, if a company wishes to export ITAR controlled software. Exports of ITAR controlled software as technical data are generally eligible for a technical data license pursuant to ITAR §125. However, the type of license required to export the software may vary depending on the scope, permanence or security level associated with the export.

Jeffrey Richardson is a senior attorney in Miller Canfield Paddock and Stone PLC's export controls group, based in Troy, Michigan. He can be reached at richardson@millercanfield.com.