MILLER CANFIELD

Are Your Software Transfers Compliant with U.S. Economic Sanctions?

January 2014

The international nature of information technology has led to the globalization of software. Globalization can have unintended negative consequences on an organization, if a company's software should find its way to a country, foreign government, or specially designated national subject to U.S. economic sanctions. These unintended negative consequences may arise whether a company's software is proprietary or developed as a product.

The U.S. government imposes economic sanctions against countries, foreign governments and specially designated nationals in furtherance of U.S. foreign policy and national security objectives. Congress has the authority to pass Economic Sanction Regulations, while the U.S. Treasury Department's Office of Foreign Asset Control ("OFAC") issues and administers these laws. OFAC can impose civil penalties up to $250,000 (USD) or twice the amount of the transaction per violation.

Currently the following countries are subject to OFAC sanctions: Balkans, Belarus, Burma,Cote d'Ivoire (Ivory Coast), Cuba, Democratic Republic of the Congo, Iran, Iraq, Lebanon, Libya, North Korea, Somalia, Sudan, Syria, and Zimbabwe.

Software Transfer Types. Software regulation under OFAC may arise through multiple types of software transfers:

- Software delivered as a physical good on a CD-ROM;
- Software downloaded by electronic transmission to the end-user;
- Software provided online in an environment hosted by the vendor; and,
- Software provided as a customized service, tailored to fit business objectives.

Software transfers may occur between software retailers, custom software developers, information technology service providers and their customers, as well as U.S. companies that develop proprietary software for use by their non-U.S. affiliates.

Location Matters. OFAC regulates software differently depending on the applicable country specific regulation, which results in different OFAC treatment for different software transfers to different country destinations.

The specific country sanctions dictate specific restrictions. For example, the Libya Sanction Regulations permit the provision of tangible goods or the conveyance of services, including Software as a Service, to individuals, except as narrowly defined in Executive Order 13566, blocking broad transfers to senior officials for the Government of Libya and the Central Bank of Libya. To contrast, the Iranian Transactions Sanction Regulations ("ITSR") prohibit the release of technology or software by a U.S. person simply "with knowledge or reason to know the technology is intended for Iran or the Government of Iran.

Similar to the ITSR, the Cuban Asset Control Regulations Sanctions ("CACR") are vastly prohibitive, precluding a property transfer to Cuba or a Cuban national by any person or business entity subject to U.S. jurisdiction, either directly or through a third country. The "property" subject to the CACR, includes "licenses affecting patents, trademarks and copyrights," "services" as well as any other property "tangible or intangible." Blocked parties under the CACR, include any person domiciled in, or a permanent resident of, Cuba, as well as any partnership, association, or

corporation organized under the laws of Cuba. Those persons or business entities subject to U.S. jurisdiction are further blocked from dealing in any property in which the Cuban Government has any interest.

The Syrian Sanctions Regulations ("SSR") block the conveyance of goods, services, software and technology to persons in Syria and those affiliated with its Government. The SSR's general information conveyance exemption permits the transfer of information including CD-ROMs, but it does not permit the transfer of supporting information incident to software exportation, if that software is subject to the Export Administration Regulations ("EAR"). Thus, even ancillary supporting information regarding EAR-regulated software remains blocked.

Screening Software End-Users. Companies can improve their compliance with OFAC Economic Sanctions Regulations by adopting an effective end-user screening program. An effective end-user screening program helps a company providing software to confirm that the software or Software-as-a-Service will not be provided to an embargoed country, specially designated national, blocked person, or ultimately for the benefit of the government of an embargoed country regulated by OFAC.

Finally, those subject to U.S. jurisdiction receiving payments from OFAC-designated countries should vigilantly confirm that OFAC permits those payments without a governmental license. If the underlying payment originates from a specially designated national or blocked party, then costly complications, including an OFAC violation, may arise, including, again, a maximum civil penalty of the greater of $250,000 or an amount that is twice the amount of the transaction that is the basis of the violation, as well as possible criminal penalties for willful violations of up to $1 million and 20 years in prison.

For further information regarding how to protect your organization from potential OFAC based software violations, we invite you to contact Miller Canfield. Visit the firm's Export Control Team's webpage for other articles and alerts, as well as updates on U.S. Export Control Reform and other export control articles.

Jeffrey G. Richardson

+1.248.267.3366