STEPTOE OUTSIDE COUNSEL

US export controls on encryption products: key points for Tech co's

US export controls on encryption products cover most types of technology – from dating apps to network servers – that contain or use cryptography and are subject to US jurisdiction. The scope of these regulations is vast, although the real-world restrictions they impose are actually quite limited in most cases. The US government achieves this purposeful dichotomy through a complex and unique regulatory structure. This article provides a step-by-step introduction for technology companies to navigate these rules.

Step 1: Do defense export controls apply to my product? The US International Traffic in Arms Regulations ("ITAR") today cover only a very narrow subset of encryption – generally military or intelligence cryptography. Most products on the ITAR's US Munitions List are controlled for reasons other than encryption. If the ITAR apply, these more restrictive rules trump the less restrictive dual-use controls under the US Export Administration Regulations ("EAR").

Step 2: Is my product excluded from the EAR because it is "publicly available"? If the code for your software is freely available without access restrictions (e.g., open source code posted to a public website), that code is considered "publicly available" and is not subject to the EAR's jurisdiction. (A notification requirement applies prior to relying on this exclusion for "non-standard" cryptography.) However, an executable software program is considered a separate EAR item, and may be restricted even if the underlying code is "publicly available". Still, the software can be excluded from EAR jurisdiction if it, too, is freely available without any restrictions on its further dissemination or access, if it uses "publicly available" code. Such "published" software may include, for example, free apps available online.

Step 3: Does my product fall into one of the substantive exclusions from the EAR's encryption controls? Even if your encryption product is subject to the EAR's jurisdiction, it may be excluded from the EAR's encryption controls. One common exclusion applies to products using cryptography for purposes other than "data confidentiality", including authentication and rights management. Another common exclusion applies to specified products with limited functionality, including smart cards, banking products, certain wireless devices, and even routers, computers and servers with certain limited cryptography. (Note that, if your product falls outside the encryption controls, it may still be subject to a non-encryption EAR restriction based on its other technical characteristics.)

Step 4: How do I know if my product qualifies for the EAR's "mass market" classification or an encryption license exception? While a licensing requirement generally applies to all countries (and their nationals), except Canada, for products and technology controlled under the EAR for encryption reasons, in practice, an exception applies in most cases. One of the most common exceptions is a classification for "mass market" products, which removes most restrictions. However, in order to trigger "mass market" treatment, you need to confirm the product is eligible under the EAR's "mass market" note and License Exception ENC, and file any required reports or classification requests to the US government. ENC is also useful for exporting most other encryption products, some after self-classification, while certain products require a formal agency classification and some reporting.

Step 5: What if my product merely incorporates a covered encryption product that performs an ancillary function? If your product does not have information security as a primary function, is not a digital communication or networking item, and is not a computer or other item with information storage or processing as a primary function (or a component of such an item), but it incorporates a cryptographic component, you should consider whether your product may be excluded from the EAR's encryption controls if both of the following are true regarding the incorporated cryptographic component: (i) it "supports a non-primary function" of your product, and (ii) as a standalone item, the component would not be subject to the EAR's encryption controls (e.g., because it has qualified for the "mass market" exception). This is an avenue for excluding many types of products that would otherwise be covered by the EAR's encryption controls.

A careful review of applicable encryption controls – highlighted in these steps – helps to avoid unnecessary delays or export penalties for product development or release. ■

About the authors:

Alex Baj is a Partner and Peter Jeydel is Of Counsel in the Washington, DC office of Steptoe. www.steptoe.com

Reprinted with permission from the September 2021 issue of Export Compliance Manager.
www.exportcompliancemanager.com