Export Group for Aerospace & Defence

Operating under the joint auspices of:

c/o ADS
"ShowCentre"
ETPS Road
Farnborough
Hampshire GU14 6FD
United Kingdom

Tel: +44 20 7091 7822
Fax: +44 20 7091 4545
E-Mail: Brinley.Salzmann@adsgroup.org.uk
URL: www.egad.org.uk

28 July 2015

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B, 14th Street and Pennsylvania Ave. NW
Washington DC 20230
United States of America
publiccommments@bis.doc.gov

RIN 0694–AG32: Revisions to Definitions in the Export Administration Regulations

Dear Sir,

I write to you on behalf of the Export Group for Aerospace and Defence (EGAD), which is a not-for-profit making special interest industry group, focusing exclusively on all aspects of export and trade control compliance matters, and is the only dedicated national industrial body in the UK dealing exclusively with export and trade control issues. EGAD operates under the joint auspices of the ADS Group Ltd (ADS), British Marine, the British Naval Equipment Association (BNEA), the Society of Maritime Industries (SMI), and TechUK.

This is in response to the consultations which were launched by the US Government on Wednesday 3rd June 2015, seeking comments on proposals for revisions to the Export Administration Regulations (EAR) to include the definitions of "technology", "required", "peculiarly responsible", "proscribed person", "published", results of "fundamental research", "export", "re-export", "release", "transfer", and "transfer (in-country)" to enhance clarity and consistency with terms also found on the International Traffic in Arms Regulations (ITAR), which is administered by the Department of State, Directorate of Defense Trade Controls (DDTC), as part of the on-going US Export Control Reform (ECR) process.

We are grateful for the high degree of constructive engagement, willingness to enter into open discussions and debate, and assistance that the US Government has unfailingly demonstrated on ECR, which have been hugely beneficial.

We would like to state that UK Industry in general is supportive of any and all efforts and initiatives associated with the ECR process to try to provide greater clarity and ease of use of US licensing. We remain committed to try to do all that we can to assist UK Industry in their understanding of the process. However we would like to submit the following comments. They relate exclusively to the new proposals relating to cryptography, set out in EAR 734.18 and the associated 764.2(l). :

a. We fully endorse the reasoning which has led BIS to propose the addition to FIPS 140-2 of 'other similarly effective cryptographic standards'. We have separately urged DDTC to adopt similar language. As non-US companies, our members operate in multiple jurisdictions. Cybersecurity and data protection are dynamic fields and national policies are constantly changing. There is always the likelihood that our domestic or international jurisdictions, as well as risk management needs, will require the use of an encryption standard that is not formally FIPS 140-2 compliant, but is similarly effective. Here in the UK, for example, companies are required to use the BeCrypt product for certain interaction with the UK Ministry of Defence. Non-US companies may also need to manage ITAR and EAR items and the different encryption rules would make developing a unified system to handle both EAR and ITAR compliance extremely challenging

b. The transfer of encrypted items in storage to restricted destinations without the owner's knowledge, should not be considered a violation by the owner. The revised EAR §734.18(a)(4)(iv) should address the scenario where properly encrypted data or software stored on a third-party's server, such as a cloud server, is transferred to a restricted jurisdiction without the permission or knowledge of the company utilizing the third party's service. As such, we suggest adding a "knowingly" standard to protect those entities that conducted due diligence in procuring third-party services from providers that do not store technical data or software in a prohibited country but whose data may end up in one of those countries without their prior knowledge or consent.

c. EAR §734.18(a)(4)(iv) includes a restriction that the unclassified technical data or software cannot be "stored" in the Russian Federation or any country listed in Country Group D:5. However the term "stored" is not defined. One would assume that this means intentional storing of information on a data server for a period of time rather than an email transiting a server and being retained temporarily for this purpose. We urge you to make clear that these country restrictions only apply to ongoing storage and not the possible transit of email through those countries. This is necessary as the sender of a secured email typically has no control over what countries an email has passed through on its way to its final destination – even emails sent between a sender and recipient in the United States may transit a third country.

d. The proposed EAR §764.2(l) states that the unauthorized release of decryption keys, network access codes, passwords, or other transfer information that would allow access to the encrypted information in clear text is an export control violation. In order to avoid any duplication of licensing, we ask that BIS make clear that existing authorizations for the export, re-export, or retransfer of information also authorize the release of decryption keys, network access codes, passwords, or other transfer information that would give access to that same controlled information to authorized parties on export license approvals. Without this clarification, companies may need to seek two separate authorizations: one that covers the export, re-export, or retransfer of controlled information and one that covers the release of decryption keys, network access codes, passwords, or other transfer information to the same authorized parties.

Thank you in advance for your consideration of these comments. If you have any questions about this correspondence please contact me.

Regards

Brinley Salzmann - Secretary, EGAD