BAE Systems plc www.baesystems.com
Warwick House, PO Box 87
Farnborough Aerospace Centre
Farnborough, Hampshire
GU14 6YU, United Kingdom

BAE SYSTEMS

3 August 2015

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
Washington, DC 20230

Via Email: publiccomments@bis.doc.gov

ATTN: RIN 0694-AG32 Revisions to Definitions in the Export Administration Regulations (80 Fed. Reg. 31505)

To Whom It May Concern:

BAE Systems plc offer the following comments in response to the request from the Bureau of Industry and Security (BIS) on June 3, 2015 (80 Fed. Reg. 31505). BAE Systems appreciates this outreach from BIS to industry and would like to take this opportunity to provide its comments to the proposed rule.

1) **Overview**. As a non-US defense industry participant in Europe, BAE Systems greatly appreciates BIS's efforts to clarify and update certain regulations related to the definitions of release, technology, and the use of encryption for the transmission of technology and software. We are largely supportive of the proposed rules, but would propose certain changes and clarification based on our experience.

2) **Release**. Under the proposed new EAR §734.15, we support the clarification of the definition of "release" so that a release only occurs when a physical, aural, or tactile inspection actually *reveals* controlled technology or source code. We understand that briefly seeing an item, such as during a plant tour, would not be sufficient to constitute a release of technology in most cases. We welcome the clarification offered by this new definition.

3) **Use of Encryption** – We are largely supportive of the proposed addition of the list of activities that are not exports, reexports, or retransfers under the EAR (§734.18). We believe that the use of secure methods of communicating technology and software should be encouraged and welcome the establishment of an agreed baseline for such encryption standards. However, we believe these proposed rules should be modified or clarified to address several key points.

   a. BIS should clarify that emails transiting a nation's internet infrastructure are not "stored" in such a country. The proposed addition of EAR §734.18(a)(4)(iv) includes a restriction that the unclassified technology 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 BIS to clarify that

these country restrictions only apply to ongoing storage and not the possible transit of emails through those countries. This clarification is necessary as the sender of a secured email typically has no control over what countries an email passes through on its way to its final destination – even emails sent between a sender and receiver in the United States may transit a third country.

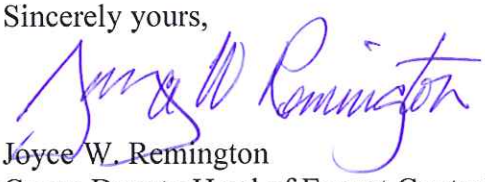
b. Encrypted items in storage should not be considered a violation where transferred to restricted destinations without a party's knowledge. The revised EAR §734.18(a)(4)(iv) should address the scenario where properly encrypted data or software stored on a third-party's server, such as a cloud server, is transferred from a permitted sender 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 technology or software in a prohibited country but whose data may end up in one of those countries without their prior knowledge or consent.

c. 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 clarify that existing authorizations for the export, reexport, 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, reexport, 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.

We hope that you will consider these alternative recommendations in the final regulation.

Thank you for your consideration of our comments.

Sincerely yours,



Joyce W. Remington
Group Deputy Head of Export Control, Licensing & Policy