ASML US, Inc.

2650 W. Geronimo Place
Chandler, AZ 85224
U.S.A.

www.asml.com

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

and

Office of Defense Trade Controls Policy
Directorate of Defense Trade Controls
Bureau of Political Military Affairs
U.S. Department of State
Washington, DC 20522

Via email: publiccomments@bis.doc.gov and
DDTCPublicComments@state.gov

Date August 3, 2015
Reference Comments in Response to Proposed Rule Makings
Subject RIN 0694-AG32 - Revisions to Definitions in the Export Administration Regulations and RIN 1400-AD70 - International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions

Ladies and Gentlemen:

ASML US, Inc. (“ASML US”) is pleased to respond to the Bureau of Industry and Security (“BIS”) and Directorate of Defense Trade Controls (“DDTC”) request for comments concerning the proposed revisions to definitions in the Export Administration Regulations (“EAR”) and International Traffic in Arms Regulations (“ITAR”).

ASML US, headquartered in Chandler, AZ, is a subsidiary of ASML Netherlands, B.V., the world’s leading provider of lithography systems to the semiconductor manufacturing industry. ASML US is the parent of Cymer LLC, headquartered in San Diego, CA, the leader in developing light sources used by chipmakers worldwide to pattern advanced semiconductor chips and is pioneering development of next generation light sources.

Rule makings RIN 0694-AG32 and RIN 1400-AD70 propose to:

(i) revise the EAR to include the definitions of ‘‘technology,’’ ‘‘required,’’ ‘‘peculiarly responsible,’’ ‘‘proscribed person,’’ ‘‘published,’’ results of ‘‘fundamental research,’’ ‘‘export,’’ ‘‘reexport,’’ ‘‘release,’’ ‘‘transfer,’’ and ‘‘transfer (in-country)’’ to enhance clarity and consistency with terms also found on the ITAR;

(ii) amend the Scope part of the EAR to update and clarify application of controls to electronically transmitted and stored technology and software; and

(iii) publish comparable amendments to the ITAR's definitions of ''technical data,'' ''required,'' ''peculiarly responsible,'' ''public domain,'' results of ''fundamental research,'' ''export,'' ''reexport,'' ''release,'' and ''retransfer'' for the same reasons.

ASML US welcomes the U.S. governments stated efforts to enhance U.S. national and economic security, facilitate compliance with export controls, update the controls and reduce unnecessary regulatory burdens on U.S. exporters. With these goals in mind, ASML US has the following comments.

I. Definitions of "Export", "Reexport" and "Release"

A. Inclusion of phrase "otherwise transferring" is confusing

ASML US has some reservations concerning the U.S. government's proposed changes to the definition of "export" and "reexport" under the EAR at § 734.13, which could be interpreted to expand the current understanding of a "deemed export," "deemed reexport" and the "release" of technology. The proposed definition of "export" in § 734.13(a)(2) reads:

> Releasing or otherwise transferring "technology" or "source code" (but not "object code") to a foreign national in the United States (a "deemed export");

ASML US believes the inclusion of the phrase "otherwise transferring" within § 734.13(a)(2) is unclear and possibly unnecessary with respect to a "deemed export". "Transfer" is defined in the EAR in the proposed rulemaking as:

> *Transfer*. A shipment, transmission, or release of items subject to the EAR either within the United States or outside the United States.

ASML US is pleased to see that the concept of "release" will be clearly expressed in a new § 734.15. The proposed addition continues to make clear the current understanding that a "release" can occur through (i) visual or other inspection; (ii) oral or written exchanges; or (iii) the application by U.S. persons of "technology" or "software" to situations abroad. However, this understanding seems somewhat at odds with the inclusion of the phrase "otherwise transfer" as it relates to "deemed export" and "deemed reexport". This is because:

- the definition of "transfer" includes the term "release", so adding "otherwise transferring" immediately after "releasing" in § 734.13(a)(2) seems somewhat duplicative; and

- as shown, a "transfer" includes a physical shipment of an item, which has not been relevant to the sharing of information contemplated by "deemed export" or "deemed reexport".

Under a strict reading of the proposed rulemaking, it appears that the mere physical shipment of "technology" or "source code" – for example on physical media such as a flash drive – to a foreign national in the United States would constitute a "deemed export" even if no actual "release" occurs. The inclusion of "otherwise transfer" seems to be an expansion of the current understanding of "deemed export", "deemed reexport" and "release". It is not clear that this is what BIS intends.

In order to avoid confusion, ASML US recommends that the U.S. government remove the phrase "otherwise transferring" from the proposed definitions of "export" and "reexport" as it relates to "deemed export" and "deemed reexport". In the alternative, BIS could use "otherwise transmitting", which seems more appropriate and removes the element of physical export from the definitions.

ASML US recognizes that BIS is creating a catch-and-release process for the "export", "reexport" or "transfer" of certain "technology". That is, BIS is capturing the "transfer" of "technology" or "software" under the definitions of "export" and "reexport" and then releasing those activities which meet the conditions set forth under the proposed § 734.18(a)(4). As a standard matter, ASML US requests that wherever BIS creates a "capture" mechanism in the EAR, that it insert a note in the regulations pointing to the relevant "release" criteria.

B. It is unclear what "software" would be captured under § 734.13(a)(6) and 734.14(a)(4)

ASML is confused by the two uses of "software" in the proposed definitions of "export" and "reexport", which because they reference a foreign national and not a consignee, appear to be directly related to a "deemed export" and "deemed reexport". This is also supported by the fact that the proposed definitions use of the phrase "'*software,'* or other information":

> § 734.13(a)(6) Releasing or otherwise transferring […] "*software*," or other information with "knowledge" that such provision will cause or permit the transfer of other "technology" in clear text or "*software*" to a foreign national**.**

and

> § 734.14(a)(4) Releasing or otherwise transferring outside of the United States […] "*software*," or other information with "knowledge" that such provision will cause or permit the transfer of other "technology" in clear text or "*software*" to a foreign national.

"Software", writ large and including object code, has not been subject to broad control under the definition of "release", "deemed export" or "deemed reexport". Instead the EAR has generally limited a "release" to "source code" as illustrated by the proposed § 734.15(a)(1) and (3):

> (1) Visual or other inspection by a foreign national of items that reveals "technology" or "source code" subject to the EAR to a foreign national;

and

> (3) The application by U.S. persons of "technology" or "software" to situations abroad using personal knowledge or technical experience acquired in the United States, to the extent that the application reveals to a foreign national "technology" or "source code" subject to the EAR.

(Section 734.15(a)(2) does not appear relevant to "software" or "source code" as it concerns the oral or written exchanges of "technology".)

ASML US therefore request that the proposed change include clarification concerning what kinds or types of "software" BIS intends to capture through the "release" of "software" that may cause or permit the transfer of other information, "technology" or "software".

In addition, to avoid confusion, BIS should consider replacing "software" with "source code" as it relates to "deemed exports" and "deemed reexports" or work through the Wassenaar Agreement process to add the particular software applications of concern to the control lists.

As written, the language is so broad that it could capture almost all electronic communication methods such as email, which can be used to transmit information that may cause or permit the transfer of other "technology" in clear text or "*software*" to a foreign national.

C. Unnecessary expansion of controls over causation and permission

ASML US believes that the addition of the phrase "will cause or permit" in § 734.13(a)(2) is overly broad. By their very nature, decryption keys, network access codes, passwords, etc., permit access to information. The very act of accessing information results in a "release", which is already a controlled activity. As a result, providing a password with "*knowledge*" that the provision will result in a release of information to a foreign national (which is the very definition of a "deemed export") just artificially doubles the number of "deemed export" transactions that occur without providing any apparent additional benefit to U.S. national security.

ASML US is additionally very concerned by the BIS's attempt to control "exports" and "reexports" which only *may* occur, as opposed to actually occurring. The proposed rule would control the provision of a password to an individual even if that password is immediately forgotten, expires and/or is simply never used.

D. Expanding controls on decryption keys and passwords would be burdensome

While ASML US believes it understands BIS's rationale for attempting to close a potential loophole concerning the release, shipment and transmission of decryption keys and passwords, it finds §§ 734.13(a)(6) and 734.14(a)(4) overly broad and potentially burdensome given that many large companies use identity management (IdM) and/or password automation systems for the generation and maintenance of access codes, passwords, etc.

ASML US, like many technology companies, controls the actual access or "release" of controlled "technology", not just the distribution of network access codes and passwords. In addition to passwords, ASML US has in place a knowledge protection program and additionally restricts access to protected technology based on, among other things, department affiliation, manager approval and a demonstrated need-to-know. As a result of this layered approach, network access codes and passwords are necessary but not sufficient to gain access to protected information. Because of this layered approach, it is not clear whether the distribution of an access code or password to a foreign national would be sufficient to meet the "will cause or permit" standard.

If the distribution of an access code or password merits control, a company may need to remove certain automated IdM and enterprise resource planning (ERP) systems and use a manual authorization process or, if possible, modify any existing systems and processes to include additional criteria such as, Country Group and license expiration dates. These types of modifications are not made quickly or easily nor are they done at a low cost in terms of money and labor resources.

In addition to these concerns, ASML US has questions concerning how this change is to be applied once a proposed change is promulgated:

- Would all current, valid deemed export and reexport licenses need to be amended to include the transfer of a decryption key, access code, password, etc., as relevant? Or would the control work in the opposite manner, that is, does a validated export license authorizing the transfer of controlled technology to a foreign national automatically authorize access to any relevant decryption key, access code or password?

- Since under the proposed rulemaking, a violation concerning the transfer of decryption keys, network access codes, passwords, etc., would constitutes a violation to the same extent as a violation in connection with the export of the controlled ''technology'' or ''software", how does one classify under the CCL an item such as hardware key fobs or token which allow for two-factor authentication. Currently such hardware is classified on

the Commerce Control List under Category 5 Part 2, but potentially enables access to technology classified under multiple categories.

- How does one classify a decryption key, access code, password, etc., if is allows access to information or technologies in clear text which are classified under multiple ECCNs?

II. Activities That Are Not Exports, Reexports, Releases, Retransfers or Transfers

A. End-to-end encryption and cloud storage

The proposed § 734.18(a) identifies a number of activities that are not treated as “exports”, “reexports” or “transfers” under the EAR. These activities subject to exclusion include sending, taking, or storing “technology” or “software” that is, among other things, secured using 'end-to-end encryption.'

While on the face of it, this exclusion from the definition of “export” and “reexport” appears useful, the reality is, it is unlikely to be broadly used. The use of end-to-end encryption greatly restricts what can be done with data that is stored, for example, in a cloud environment. Information, once encrypted, cannot be easily indexed, queried, retrieved or manipulated, which removes much of the utility and benefit from enterprise cloud storage.

Nevertheless, ASML US believes this exclusion is a positive step in the U.S. government’s understanding and treatment of the use of encryption by industry.

B. Activities That Are Not Deemed Reexports

ASML US is very pleased to see BIS promulgate its current guidance concerning “deemed reexports” in the EAR. However, ASML US would like BIS to provide additional clarification in the regulations concerning when the proposed exclusions at § 734.20(a), (b) and (c) are applicable particularly when License Exception Technology and Software Under Restriction (TSR) is available to a foreign national who is either of a country that is identified:

- under Country Group B *and* Country Group A:5 (such as the Netherlands); or
- under Country Group B *and* a country *not* identified under Country Group A:5 (such as Brazil).

Under § 734.20(a), a foreign entity would only need to be certain that the foreign national’s most recent country of citizenship or permanent residency is that of a country to which export from the United States of the ‘‘technology’’ or ‘‘source code’’ at issue would be authorized by, for example License Exception TSR. However, under § 734.20(b) and (c), a foreign entity would need to comply with many additional requirements.

Also, in order to avoid confusion and unnecessary submissions of license applications to BIS, ASML US recommends that a note be inserted in the definition of “deemed reexport” at § 734.14 which point to § 734.20.

* * *

ASML US greatly appreciates the opportunity to comment on the proposed rulemaking and looks forward to continuing its cooperation with the U.S. government on export control reform.

Sincerely,

Steve Lita
Manager, Export Compliance