Yale OFFICE OF THE VICE PRESIDENT
AND GENERAL COUNSEL

PO Box 208255
New Haven CT 06520-8255
T 203 432-4949
F 203 432-7960

courier
Whitney Grove Square
2 Whitney Avenue, 6th Floor
New Haven CT 06510

August 3, 2015

Ms. Hillary Hess
Director
Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
Washington, D.C. 20230

Dear Ms. Hess:

I write on behalf of Yale University to comment on the Bureau of Industry and Security's (BIS) proposed revisions to the definitions in the Export Administration Regulations (EAR).

Yale applauds this important effort to make the language and structure of EAR and the International Traffic in Arms Regulations (ITAR) more consistent, thereby achieving greater harmonization of two distinct regulatory regimes. In general, we believe this is a positive step toward implementation of the Administration's Export Control Reform Initiative – and the ultimate export control objective of creating a common set of regulations. With careful construction and implementation, these reform efforts will enhance national security and facilitate compliance while reducing related costs and burdens for exporters, including Yale.

We appreciate that most of the proposed revisions would not substantively change the existing rules. Instead, they would create substantive and structural harmonization, using the same words for the same concepts in the EAR and ITAR and similar definitions in a common format that helps make the differences clear. In particular, we support proposed inclusion of the definition of fundamental research proposed by the BIS in Section 734.8(c), which is identical to the National Security Decision Directive (NSDD) 189. To smooth implementation and aid in compliance, we suggest revisions or clarifications to the sections concerning the end-to-end encryption standard, the definitions of "technology" and "software," and the contract controls for government-sponsored research.

Fundamental Research Definition

We support the proposed definition offered by BIS for 'fundamental research', which we believe is identical to the definition in NSDD-189. Specifically, in Section 734.8(c), 'fundamental research' means "basic or applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community." The use of this definition in the EAR and the ITAR would be most consistent with our understanding of

the term. We also believe this is an improvement over the alternative proposed definition, in which 'fundamental research' means "non-proprietary research in science and engineering, the results of which are ordinarily published and shared broadly within the scientific community." We are concerned that the alternative definition relies on undefined or vague terms. For example, the term 'non-proprietary' could be defined to mean several different things, including unprotected by patents, copyrights or trademarks or existing in the public domain.

Fundamental Research and Software

Currently, the EAR, in Section 734(b)(3), states that "publicly available technology and software...[that] arise during, or result from, fundamental research" are not subject to the EAR. Yet, as proposed in Section 734.8, only 'technology' that arises during, or results from, fundamental research and is 'intended to be published' would not be subject to the EAR. Further, the preamble discussing this section states that the "proposed notes clarify that...software and commodities are not 'technology resulting from fundamental research.'" In other words, in the above referenced sections, software appears to be no longer covered by the fundamental research exception.

Notwithstanding these sections, the general section on exclusions would seem to contradict the proposed narrowing of the fundamental research exception, creating tension and confusion. Specifically, proposed Section 734.3(b)(3) states that "information and 'software'" are not subject to EAR if they arise during, or result from, fundamental research, as described in Section 734.8.

If software arising during, or resulting from, fundamental research were no longer subject to the fundamental research exception, research at Yale would be significantly constrained. Natural language documents written by a researcher may be considered "technology" while a computer language document written by the same researcher may be considered "software." Despite the fact that both arise during fundamental research and are written for the purpose of being freely shared, the technology would be considered exempt while software would be subject to deemed export restrictions. This conclusion would be at odds with the fact that much of science involves the creation of software. If such software were no longer covered by the fundamental research exception, Yale would have to treat the research itself as not covered, undercutting the value of the exception and potentially subjecting much of our research to export controls. Given that the export definitions in Section 734.2(b) recognize the similarities between software and technology, and the confusion that this change will likely cause, we strongly recommend that software arising during, or resulting from, fundamental research remain covered by the fundamental research exception.

Further, we have noticed that the current presumption in EAR 734.8(b), that university-based research is considered fundamental research, appears to have been eliminated. Absent a clear policy reason for this change, we urge you to restate the presumption in the final rule.

Transfer and Storage

The proposed rule clarifies that when technology/technical data or software is transmitted electronically through, or stored electronically in, a foreign country, an export, reexport, or (re)transfer has <u>not</u> occurred if the technology/technical data or software is unclassified; it is encrypted end-to-end; it is secured using modules compliant with FIPS 140-2 and supplemented

by other controls consistent with NIST guidance; and, in the case of technical data under ITAR or controlled technology or software under EAR, it is not stored in a proscribed country listed in Section 12.1 or in Country Group D-5 or in Russia.

We greatly appreciate the proposed rule's clarification that the transmission of unclassified technical data through a foreign country's Internet service infrastructure does not require a license, provided that the technical data is encrypted prior to leaving the sender's facilities and remains encrypted until received by the intended recipient. Similarly, we appreciate that the electronic storage abroad of encrypted technical data would not require an authorization. As you have recognized, ITAR controlled technical data may be electronically routed through foreign servers without the knowledge of the original sender. For example, an email may, without the sender's knowledge, transit a foreign country's Internet service infrastructure en route to its intended destination. Or data intended for cloud storage may, without the sender's knowledge, be physically stored on a server located in a foreign country (or multiple foreign countries). This creates a risk of unauthorized access and a potential for an inadvertent ITAR violation, which the proposed rule seeks to mitigate.

Even with the improvements in the proposed rule, we are concerned that the end-to-end encryption requirement will create significant compliance challenges for institutions that rely on third party vendors for these services. As stated above, these servicers might encrypt and decrypt information at various points in the process of transmitting or storing technology or software, potentially triggering an export or reexport that would require BIS authorization. Although not explicitly stated in the proposed rules, the end-to-end encryption requirement seems to imply that the owner of the data or software (the sender), not the vendor, would be responsible for any unauthorized transmission or release of controlled technology or software. Given that vendors ultimately will be responsible for refining their offerings to ensure that data is not decrypted at any time and that no servers are located in restricted countries, we urge you to consider the creation of a safe harbor for senders that impose a contractual obligation on the vendor to comply with these transmission and storage requirements.

In addition, with respect to the intended control, we prefer the proposed EAR definition in 734.13(a)(6), which requires knowledge that releasing information relating to encryption will cause or permit the transfer of technology to a foreign national. In general, knowledge or intent to transfer controlled information should be required for an "export" or "deemed export" to occur.

Ultimately, the usefulness of the transfer and storage provisions in the proposed rule will be limited by the prohibited countries list. We strive to clearly understand what is going to happen to our data once it is in the cloud (i.e. what data will be uploaded, transferred or downloaded from the cloud, and when and by whom) and we take steps to ensure that providers put appropriate measures in place to prevent unauthorized access, but many large providers are unwilling to tell users where their clouds are located or on which clouds data is stored. Given that the burden of compliance rests with the sender, not the provider of the cloud computing services, the inclusion of China in a prohibited county list would effectively preclude U.S. institutions and companies from using cloud storage. We urge you to consider a narrower prohibited countries list – such as the Office of Foreign Assets Control embargoed countries list - that, together with end-to-end encryption, will provide adequate protection without requiring compliance with mandates that are outside of the sender's primary control.

Contract Controls/Government Sponsored Research

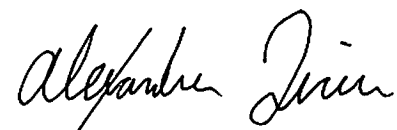
Currently, Section 734.11 provides: "If research is funded by the U.S. Government, and specific national security controls are agreed on to protect information resulting from the research, the provision of Section 734.3(b)(3) will not apply to any export or reexport of such information in violation of such controls. However, any export or reexport of information resulting from the research that is consistent with the specific national security controls may nonetheless be made under this provision." The proposed EAR rule restates the current 734.11(a), which always has been a source of confusion, with the meaning of "this provision" in the last sentence unclear.

The Q&A embedded in the current regulations make clear that any export "that is consistent with the controls will continue to be eligible...under the 'fundamental research' rule." (Supplement No. 1 to Part 734, Question E(1)) With the Q&A being moved out of the regulation, we believe it is important to make sure that Section 734.11 is unambiguous. Therefore, we suggest the following modification:

> "If research is funded by the U.S. Government, and specific national security controls are agreed on to protect information resulting from the research, the provision of Section 734.3(b)(3) will not apply to any export or reexport of such information in violation of such controls. However, any export or reexport of information resulting from the research that is consistent with the specific national security controls may nonetheless be made under Section 734.3(b)(3)."

Again, we appreciate this opportunity to comment. We look forward to working with you to preserve the U.S. leadership position in science and technology and to advance the national security.

Sincerely,



Alexander Dreier
Vice President and General Counsel