AAU *Association of American Universities*
APLU *Association of Public and Land-grant Universities*
COGR *Council on Governmental Relations*

August 3, 2015

Rose Gottemoeller
Under Secretary for Arms Control and International Security
Office of Defense Trade Controls Policy
Department of State
2401 E. Street, N.W.
Washington, D.C. 20037

Via Email: DDTCPublicComments@state.gov

Re: ITAR Amendment—Revisions to Definitions; Data Transmission and Storage (RIN 1400—AD70)

Dear Under Secretary Gottemoeller:

Enclosed please find comments from the Association of American Universities, the Association of Public and Land-grant Universities, and the Council on Governmental Relations on the ITAR Amendment – Revisions to Definitions; Data Transmission and Storage (RIN 1400-AD70). Our staff is available to provide more information or discuss these matters further should you have any questions regarding our comments.

Sincerely,

Hunter R. Rawlings III
President
AAU

Peter McPherson
President
APLU

Anthony DeCrappeo
President
COGR

Attachment 1

AAU *Association of American Universities*
APLU *Association of Public and Land-grant Universities*
COGR *Council on Governmental Relations*

MEMORANDUM

August 3, 2015

TO: **Office of Defense Trade Controls Policy, U.S. Department of State**

FROM: **Association of American Universities**
Contact: Tobin Smith, toby.smith@aau.edu (202) 408-7500
Association of Public and Land-grant Universities
Contact: Jennifer Poulakidas, jpoulakidas@aplu.org (202) 478-5344
Council on Governmental Relations
Contact: Robert Hardy, rhardy@cogr.edu (202) 289-6655

Re: **(RIN 1400—AD70)**
ITAR Amendment—Revisions to Definitions; Data Transmission and Storage

On behalf of the over 200 universities represented by our associations, we greatly appreciate the opportunity to comment on the revisions to ITAR definitions and concerning data transmission and storage (RIN 1400—AD70).

The Association of American Universities (AAU) is an association of 60 U.S. and two Canadian leading research universities organized to develop and implement effective national and institutional policies supporting research and scholarship, graduate and undergraduate education, and public service in research universities. The Association of Public and Land-grant Universities (APLU) is a research, policy, and advocacy organization of 238 public research universities, land-grant institutions, state university systems, and affiliated organizations, dedicated to increasing degree completion and academic success, advancing scientific research, and expanding engagement. The Council on Governmental Relations (COGR) is an association of 190 U.S. research universities and their affiliated academic medical centers and research institutes that concerns itself with the impact of federal regulations, policies, and practices on the performance of research and other sponsored activities conducted at its member institutions.

The proposed ITAR rule contains a number of helpful changes and clarifications (e.g. definition of "release," clarification that submission of manuscripts to journal editors constitutes "published" information). In addition, we appreciate the Department's repeated attempts to clarify the definition and scope of "defense services." This has been a longstanding issue of concern to our members. Unfortunately, there is one particular aspect of the proposed changes which we believe will largely over shadow these other positive changes.

The proposed ITAR rule would consider any proprietary information review requirement imposed by a sponsor to exclude this research from being considered fundamental, even when ultimately no information is deemed to be proprietary. This is extremely problematic and threatens to stifle university-industry research collaborations. *We therefore strongly urge DDTC to eliminate the language excluding information subject to proprietary review from being considered fundamental research and to align its language more closely with the EAR treatment of data where a sponsor requires prior review before publication.*

Prepublication Review

We appreciate that the proposed ITAR rule recognizes that information arising during, or resulting from fundamental research that is intended to be published is not technical data subject to the ITAR (and now provides a separate definition apart from "public domain" for fundamental research information). Currently the ITAR does not directly address this point.

However, the proposed rule (120.49(b) provides that "intended to be published" does not apply to research sponsor proprietary information review. In order to be considered fundamental research a researcher must be free to publish the information without any restriction or delay. This is a marked contrast from the EAR, which continues to provide that such review does not change the status of technology that arises during or results from fundamental research as still "intended to be published."

Under the proposed ITAR rule, all research agreements that involve defense articles subject to the ITAR in which publication is subject to a proprietary information review by the sponsor would not be considered fundamental research. Control plans and licenses for any foreign nationals involved in such activities would be required before projects could be undertaken.

No explanation is provided as to the reason for these different policies. The ITAR provision contradicts the intent of the reform initiative to harmonize the EAR and ITAR. More importantly, it will have a chilling effect on university-industry collaborations directly working against the Administration's efforts to increase these types of collaborations to more quickly move new ideas from the lab to the marketplace. Almost all agreements with industry sponsors include provisions for proprietary and patentable information review. Companies understandably want the ability to guard against inadvertent disclosure of their proprietary information or trade secrets in publications of research findings and results by university researchers. Without this ability industry is unlikely to enter into sponsorship of university research. However, there still is a clear intent to publish the research results. The purpose of these short-term (typically 30—60 days) delays for review is to ensure that any proprietary input data received from an industry partner is not included inadvertently in an academic publication. Such clauses do not imply in any way that the research results themselves would somehow be proprietary to the company. In fact, often universities routinely include a clause that reinforces the fact that they are academic institutions that have the right to publish research results. This situation differs significantly from situations where the sponsor must approve publication of the research results. Many universities will not accept such terms from sponsors, in large part because they are not considered fundamental research.

Universities and their faculty are being pushed by government at all levels, including the Federal government, to increasingly collaborate and work more closely with industry in an effort to quickly move products from the lab to the marketplace. Our member institutions are very aware of the need to meet these challenges while preserving the open nature of university research. The proposed ITAR provision is counter to these goals and threatens the ability of universities to achieve these objectives, particularly in defense-related areas where universities often serve as subcontractors to defense contractors for research related to particular defense technologies. It is unclear how treatment of such activities as controlled serves our national security interests. Additionally it clearly does not serve our economic interests. We have worked extensively with the Department of Defense to ensure that neither government nor sponsor approval is required for publication of fundamental research findings in such situations. Requiring licenses and control plans for research projects which are merely subject to sponsor review for proprietary information - but for which in most cases no proprietary information is in fact included - will greatly increase compliance burdens, and adversely affect the interest and ability of universities to undertake such research projects.

The proposed rule also raises serious questions of consistency with government policy on the transfer of scientific and technical information as reflected in National Security Decision Directive 189 (NSDD 189). That directive provides that "No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. statutes." It also provides that "…to the maximum extent possible, the products of fundamental research (should) remain unrestricted." The proposed

rule restricts research where the results are merely reviewable by sponsors for the possible erroneous inclusion of proprietary information. This appears an arbitrary agency decision lacking clear statutory authorization in contravention of stated government policy. We strongly urge that "…or research sponsor proprietary information review" be deleted from the proposed 120.49(b).

Fundamental Research

There is an inconsistency between the proposed §120.49 entitled "Technical data that arises during, or results from, fundamental research," and 120.6 (a)(3) which indicates that information and software that arise during, or result from, fundamental research, are not subject to the ITAR. The proposed definition of "technical data" in 120.10(a) includes information but not software. This appears to be a significant narrowing of "fundamental research." Omission of software from "fundamental research" would significantly complicate and restrict university research. While natural-language documents written by a researcher would be "technical data" that could be freely shared as arising during fundamental research, a computer-language document written by the same researcher, working on the same project (a program in source code) would be subject to deemed export restrictions. Information and software are treated the same way in the proposed definition of "public domain" (120.11) and deemed export (§120.17(a)(2)). We believe that 120.49 should be revised to apply clearly both to technical data and software.

In addition, Note 1 to paragraph 120.49(a) states that "The inputs used to conduct fundamental research, such as information, equipment, or software, are not "technical data that arises during or results from fundamental research" except to the extent that such inputs are technical data that arose during or resulted from earlier fundamental research." We believe the statement may be misleading. Conduct of fundamental research draws upon a wide range of information and other inputs. NSDD 189 does not make a distinction between the conduct and results of fundamental research, In drawing such a sharp distinction, DDTC appears to be arbitrarily restricting NSDD 189 without clear authority. We question the need for this statement, and urge that it be removed.

Defense Services

We appreciate the attempt to provide a narrower definition of "defense service," and concur with DDTC that the revised definition is unlikely to encompass normal duties of university employees. However, in the course of considering the public comments on the several previous definitions proposed for "defense services," DDTC appears to have gone somewhat to the opposite extreme in the proposed 120.9(a)(1) and now has decoupled the actual use of technical data in providing the defense service. Instead it is based on knowledge gained through participation in the development of defense articles. We believe such a subjective test will be difficult to apply in practice both for the regulated community and DDTC. There needs to be a clear connection to using the technical data in providing the assistance.

We also appreciate the distinction between "integration" and "installation" in 120.9(a))(2), which appears consistent with our previous comments on this issue. However, it appears that use of public domain information in "integration" still may be a defense service. We believe performing a defense service should be tied to use of technical data, regardless of whether it involves integration or furnishing of other assistance. We are concerned that with the new proposed definition of "integration," (a)(2) could encompass normal sharing of academic information.

We suggest DDTC consider harmonizing the education exclusion now in the proposed 120.9(a) Note 9, with the proposed revised EAR 734.3(b)(3)(iii), which merges current ITAR (120.10(b)) and EAR text. We further suggest that the language "or by instruction in a catalog course or associated teaching laboratory of an academic institution" be added to avoid unintentionally limiting this exclusion. University courses in emerging technology areas should be covered so long as they are included in course catalogues. It also would be helpful to add a note that university capstone project courses are not considered defense services.

Public Domain

The proposed ITAR 120.11 revises the definition of "public domain" to identify characteristics without limiting the definition to specific circumstances as in the current ITAR. While we agree with the intent to streamline the definition, the examples given still are primarily in terms of tangible information and do not at all recognize newer forms of information technology such as photonics. The same comment applies to other ITAR provisions, e.g. 120.17.

The provision in the proposed 120.11(b) that technical data or software is not in the public domain if it has been made available to the public without authorization from the government raises serious concerns for us. It may lead to confusion over how this provision applies to information made available to the public through any of the means listed in 120.11(a). It is not clear how data or software that already has been publicly shared through one or more of these means cannot be considered as in the public domain. No time limit is indicated in 120.11(b). Moreover the scope is not limited to government funding, and could apply to a very wide range of unclassified information from many different sources. This provision raises serious legal and policy issues. We urge DDTC to withdraw it or substantially limit its scope. Corresponding changes should be made to the proposed 127.1(a)(6). As stated this provision raises questions as to who in the chain of making technical data or software publicly available would be held responsible and what type and degree of knowledge is required for violations.

Cloud Computing

We appreciate that both the proposed EAR and ITAR rules address cloud computing situations, which have been a cause for considerable uncertainty under the current rules. In the companion rule BIS asks for comments as to which proposed rule more clearly describes 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, we believe that knowledge or intent to transfer controlled information should be required for an "export" or "deemed export" to occur. We also prefer the EAR provision in 734.18(4)(iii) providing for “other similarly effective cryptographic means “ for securing technology or software to the proposed ITAR 120.52(a)(4)(iii). While the NIST standards are widely accepted, they are not necessarily followed by all our member institutions since some institutions use other means to assure effective cryptographic management.

In addition, the restriction in 120.52 (a)(iv) to countries not proscribed in 126.1 unfortunately may substantially limit the usefulness of the proposed rule. In the experience of our members, most cloud providers insist on storing data anywhere that they want. We suggest DDTC consider adding a note that a contract that imposes these obligations on a vendor is sufficient for compliance purposes, to provide a greater safe harbor. Ensuring actual compliance is beyond our members' control.

Other Comments

DDTC asks for comments on the technical aspects of data transmission and storage in 120.17. Our associations are unable to comment on these aspects, but we have encouraged our members to do so.

Note 3 to the new definition of "Required" in 120.46(a) provides a definition for "peculiarly responsible" identical to the proposed stand-alone EAR definition in 772.1. DDTC asks for comments on placement of this definition. The EAR placement seems easier to identify, but we have suggested that our members provide their own review and comments on this issue.

We also suggest that DDTC add a note to the proposed 120.47 definition of “development” to clarify that prototypes fabricated by universities solely for academic demonstration purposes with no intent to develop them for commercial production are not “development.”

Effective Date

DDTC proposes a 30-day delayed effective date. Changes to USML categories generally have had a six-month delayed effective date while other rules affecting export controls have been effective on the date of publication. Obviously the content of the final rule is an important consideration. Our view is that significant changes in definitions should have as long a lead time as possible for implementation. Therefore we support a six-month delayed effective date.

Conclusion

In closing, we believe there are many positive changes in the proposed rule. Unfortunately they are overshadowed by the proposed 120.49(b) prepublication review restriction discussed above. We strongly urge DDTC to reconsider this restriction, which is inconsistent both with stated government policy on fundamental research and on current government policy objectives as well as the goals of the export controls reform initiative to harmonize definitions.

We appreciate the opportunity to comment and are available to provide more information or discuss these matters further should you have any questions regarding our comments.