

American Council on Education



Office of the President

October 12, 2005

Defense Acquisition Regulations Council
Attn: Ms. Amy Williams
OUSD (AT&L) DPAP (DAR)
IMD 3C132
3602 Defense Pentagon
Washington, DC 20301-3062

RE: DFARS Case 2004-D010 (Export-Controlled Information and Technology)

Dear Ms. Williams:

On behalf of the members represented by the American Council on Education (ACE) and the National Association of Independent Colleges and Universities (NAICU), we are pleased to submit the following comments in response to the proposed rule published on July 12, 2005 in the *Federal Register* seeking public input on certain amendments proposed by the Department of Defense to the Defense Federal Acquisition Regulations Supplement (DFARS) to prevent the unauthorized disclosure of "export-controlled information and technology" under Department of Defense contracts.

ACE and NAICU acknowledge the importance of protecting sensitive information and data from unauthorized disclosure, and supports the Department of Defense's efforts to include standard provisions in defense contracts that put contractors on notice of their obligations that may arise under U.S. export control laws and regulations. However, we respectfully submit that the proposed rule, as written, raises questions about the treatment of the long-standing exception for "fundamental research" under U.S. export control laws, and imposes new regulatory burdens on academic researchers that do not provide any obvious national security benefits.

I. Proposed Rule on "Export-Controlled Information and Technology"

The July 12, 2005 proposed rule requires Defense Department contracting officers to ensure that contracts identify any "export-controlled information and technology" that will be used or generated in performance of such contracts. It also sets forth a standard export control-related clause for use in solicitations and contracts for research and development or for services and supplies that may involve the use or generation of "export-controlled information and technology." That clause requires the contractor to:

- (i) comply with all applicable laws and regulations regarding "export-controlled information and technology";
- (ii) maintain an "effective" export compliance program, apparently regardless of whether the contract involves "export-controlled information and technology";
- (iii) conduct initial and periodic training on export compliance controls; and
- (iv) perform periodic assessments to ensure full compliance with U.S. export control laws and regulations.

The proposed rule imposes these contract requirements on all subcontractors, regardless of whether the subcontractors deal with controlled information or technology. Not all defense contracts involve export-controlled information and technology.

RE: DFARS Case 2004-D010
October 12, 2005
Page 2

The proposed rule was ostensibly drafted to respond to the Department of Defense Office of Inspector General's ("OIG") March 25, 2004 report on "Export-Controlled Technology at Contractor, University, and Federally Funded Research and Development Center Facilities (D-2004-061)." In that report, the OIG found that the Defense Department did not have adequate processes to identify unclassified export-controlled technology and to prevent unauthorized disclosure of such information to foreign nationals. It recommended that the DFARS be amended to incorporate Federal export control laws and regulations, and that contracting officers include such requirements in defense contracts. The report did not suggest amending the DFARS to limit the applicability of the fundamental research exception to contractors or to impose new obligations on contractors that engage solely in fundamental research.

II. Importance of Fundamental Research and Export Controls

Many of the universities and academic research institutions that we represent are involved in contracts with the Department of Defense, including conducting fundamental research in partnership with the U.S. Government. University-based basic and applied research is a vital component of our national and economic security, and contributes to U.S. preeminence in science and advanced technology. The Department of Defense's proposed amendments to the DFARS with regard to "export-controlled information and technology" have a direct impact on the ability of American colleges and universities to conduct fundamental research and achieve breakthroughs in science and technology, and thus have important implications for national and economic security and the nation's continued leadership in science and advanced technology.

ACE and NAICU acknowledge the importance of ensuring that sensitive information and technology generated or shared pursuant to a defense contract are not diverted to unauthorized end-users for unauthorized purposes. Indeed, many organizations representing universities and academic research institutions have been engaged in an unprecedented effort to educate academic researchers about their obligations under U.S. export control laws and regulations, and are working with the Department of Commerce to share information about the impact of such laws and regulations on the academic research community. While we support the Department of Defense's efforts to promote compliance with U.S. export control laws and regulations, we note that not all defense contracts involve export-controlled information and technology. In addition, many defense contracts with universities fall within the well-established exception for fundamental research under U.S. export control laws and regulations.

III. Concerns About the Proposed Rule

We respectfully submit that the proposed rule as written raises questions about the long-standing exception to U.S. export control restrictions for fundamental research that need to be clarified in the final rule. The proposed rule does not make reference to standing Presidential policy on federally-funded fundamental research (NSDD-189), which states that "to the maximum extent possible, the products of fundamental research remain unrestricted." Also, in its current form, the proposed rule imposes additional regulatory burdens on academic researchers that do not provide any appreciable national security benefits.

First, the proposed rule could be read to subject information or technical data related to fundamental research to new export control restrictions. Under the Export Administration Regulations ("EAR") and the International Traffic in Arms Regulations ("ITAR"), information or technology meeting the definition of fundamental research are exempt from export control requirements.¹ The proposed rule, however, does not exclude fundamental research from its definition of "export-controlled information and technology," and, therefore, implies that fundamental research is "export-controlled."

As the proposed rule states that its provisions are not intended to change or supersede the EAR and ITAR, we assume that the Defense Department did not intend to restrict the application of the fundamental research exception when the terms of the exception are met in the performance of a defense contract. In the final rule, the

¹ See 15 C.F.R. §734.8 and 22 C.F.R. §120.11(a)(8), §125.1(a).

RE: DFARS Case 2004-D010
October 12, 2005
Page 3

Department of Defense should clarify the treatment of fundamental research by applying the rule only to information and technology "subject to the EAR or ITAR." This formulation would ensure that fundamental research and other information that is exempted under the EAR or ITAR are not subject to the new requirements.

Second, the proposed rule appears to require all contractors to maintain an "effective export compliance program," regardless of whether the contract involves information or technology subject to the EAR or ITAR. This means that universities or colleges will be required to put in place an export control compliance system, including an access control plan, unique badging requirements, periodic training, and auditing, even though the contract does not involve any restricted information or technology, as is the case with fundamental research. Establishing such a compliance system would require universities to devote substantial resources to hiring additional compliance personnel to implement the program, conducting specialized training for researchers and support staff, implementing systems for monitoring and tracking foreign-national researchers, and creating procedures to identify controlled items and obtain required authorizations from the U.S. Government. Such requirements would impose excessive administrative and regulatory burdens on universities or colleges that normally do not deal with controlled information or technology, with no obvious benefit to national security.

In addition, by requiring all contractors to implement export control compliance programs, this provision imposes additional requirements on contractors beyond what is required under the EAR or ITAR. While the Departments of Commerce and State recommend certain guidelines for export compliance programs, neither the EAR nor the ITAR require exporters to have such programs in place. The proposed rule also does not identify any criteria or process for determining whether an export compliance program is "effective," and does not discuss who will make such judgments. If the Department of Defense is to make such judgments, there is no indication of whether the Department of Defense will ensure that its determinations are consistent with the guidelines used by the Departments of Commerce and State for compliance programs.

As a general matter, the proposed rule establishes a parallel set of export control requirements enforced by the Department of Defense that unnecessarily duplicate the efforts of other agencies, including the Departments of Commerce and State. Under the proposed rule, in addition to complying with the EAR and ITAR, universities and other academic research institutions will be required to comply with requirements under the DFARS to identify controlled information in contracts, establish "effective" compliance programs, conduct training, and assess compliance efforts. This redundancy is particularly problematic if the Department of Defense uses standards to enforce its DFARS provisions that are different from the standards used by the State and Commerce Departments with regard to their regulations.

IV. Suggested Approach for Protecting Controlled Information

In light of the above, rather than creating a parallel regime, we recommend that the DFARS be amended only to require the inclusion in defense contracts of a standard clause that expressly makes contractors aware of their obligations, if any, under the U.S. export control laws and regulations. Such a clause could include the following language:

- (a) In performing this contract, the Contractor may need to export information, technology, software, equipment, and other items subject to the Export Administration Regulations (EAR) (15 CFR Parts 730-774) or the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130). The transfer of such items to foreign persons in the United States or the export of such items to foreign destinations may require prior authorization from the Department of Commerce or Department of State, or may be subject to other requirements under the EAR or ITAR.
- (b) It is the responsibility of the Contractor to comply with the U.S. export control laws and regulations, including the EAR and ITAR, to the extent they apply to the performance of this contract.

RE: DFARS Case 2004-D010
October 12, 2005
Page 4

- (c) If the Department of Defense or any other organization acting on behalf of the Department of Defense intends to transfer any export-controlled information, technology, software, equipment, or other items subject to the EAR or ITAR to the Contractor during the performance of this contract, the Department of Defense will identify in the contract the specific Export Control Classification Numbers (ECCNs) and/or U.S. Munitions List categories of those controlled items.

Under this formulation, contractors would not be required to duplicate efforts by also working with the Defense Department to implement export compliance programs. Rather, contractors would be put on notice that they must work with the appropriate agencies to identify controlled commodities or technology used or generated in performance of the contract, and obtain any required authorizations. In addition, in contracts where the Defense Department expects to transfer controlled information or technology to the contractor, the Defense Department would identify such information or technology by its ECCN or U.S. Munitions List category in the contract.

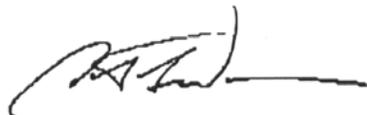
We believe that the EAR and ITAR adequately protect against the unauthorized disclosure of controlled information or technology, and that there is no need to create a redundant, parallel export control regime enforced by the Department of Defense. The approach we are suggesting also would not create new, burdensome obligations for universities and other academic institutions engaged in fundamental research that is exempted from export control requirements under the EAR and ITAR.

ACE and NAICU recommend that the proposed rule be modified to incorporate the suggestions made in this submission.

Respectfully submitted,



David Ward
President
American Council on Education



David Warren
President
National Association of Independent
Colleges and Universities

DW/cms