

AAU Association of American Universities
COGR Council on Governmental Relations

February 29, 2016

Mr. Dustin Pitsch
Defense Acquisition Regulations System
OUSD (AT&L) DPAP/DARS, Room 3B941
3060 Defense Pentagon
Washington, D.C.20301-3060

Re: DFARS Case 2013-D-018

Dear Mr. Pitsch:

On behalf of the Council on Governmental Relations (COGR) and the Association of American Universities (AAU), we write to comment on the subject DFARS case. 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. AAU is an association of 60 U.S. and two Canadian preeminent 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.

We appreciate DOD's responsiveness to the concerns expressed in our previous comment letter about the compliance burdens associated with the new safeguarding requirements in the revised DFARS 252.2004—7008 and 7012 clauses. As stated in the December 30, 2015 Federal Register Notice, the revised clauses relieve contractors of the requirement to immediately implement the NIST requirements. While our concern about the long-term burdens remains, the delay in the required implementation of the NIST SP 800-171 requirements to December 31, 2017 will be helpful to our member institutions in assessing and planning for needed changes in their current information systems.

We note, however a seeming contradiction between the revised 7008 and 7012 clauses. The 7008 clause requires contractors to represent by submitting offers that they will implement the requirements by that date. If a contractor proposes to vary from any of the NIST requirements, a written explanation must be submitted to the DOD Chief Information Officer (CIO) either as to why the requirement is inapplicable or how an alternative but equally effective measure will be used. The CIO representative will adjudicate variance requests prior to contract award.

In contrast, the 7012 clause requires notification of the CIO within 30 days of contract award of any NIST requirement that has not been implemented or of alternative measures to achieve equivalent protection that have been accepted in writing by the CIO. According to the Federal Register Notice, this will help DOD monitor progress and identify trends in implementation that may require clarification or adjustment. This appears to result in a contradiction between the two clauses. The discussion in the Notice specifically states that the requirement for CIO acceptance is removed in the 7012 clause. There appears to be little incentive for contractors to obtain CIO acceptance if a notification only is required prior to the December 31, 2017.

We understand that under both clauses contractors either must obtain variances or fully implement the NIST requirements by that date. However, the present wording is likely to result in confusion. We suggest that DoD clarify the intent of the notification requirement.

Our other concern involves the applicability of the requirements to contracts determined to be fundamental research under DFARS 7000(a)(3). Our understanding is that the 7008 and/or 7012 clauses will be included in such contracts from DOD agencies. In our previous comments we had expressed concerns that our member institutions who solely conduct fundamental research with DOD funding not become inadvertently subject to the new requirements. We urged DOD to include both in the policy guidance and the 7008 clause a provision that projects determined to be fundamental research do not involve covered defense information subject to the safeguarding requirements. We again urge DOD to include this clarification in the DFARS.

Such a clarification could take two forms. First, the definition of “export control” contained in 48 C.F.R. § 204.7301, §252.204-7008(a) [through the definition of “covered defense information”], §252.204-7009(a)(2)(iii), and §252.204-7012(a)(ii)(C) describes unclassified information concerning certain items, commodities, and technology. The definition continues: “To include dual use items; items *identified in* export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.” (Emphasis added.) The regulations referenced in the definition contain protections for fundamental research that do not appear on the face of the definition even though it is our understanding that DOD does not intend to change the current legal standard for export controlled information. We believe that problem could be addressed by a relatively straightforward revision: changing the reference from information “identified in” to information “subject to” the export control regulations.

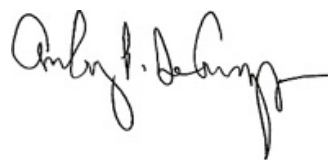
We therefore recommend this definition be revised as follows:

Export control. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives and that is subject to U.S. export control laws and regulations.

Second, we appreciate that DOD has determined that the subcontractor flow down requirement in §252.204-7012 should apply only to those subcontractors whose efforts will involve covered defense information or who will provide operationally critical support. This ensures that universities engaged in fundamental research are not required to conform to the 7012 requirements. We believe that this same approach should be applied to prime contractors whose work will not involve the use of covered defense information. That is, 7012 should be revised to state that where the contractor is neither expected to receive or produce covered defense information, the 7012 requirements will not apply until such time as covered defense information is received or produced. Such a revision would allow fundamental research to proceed without the safeguarding measures that are inapplicable to such research while still ensuring that the necessary measures are triggered should covered defense information become involved in the project at some point in the future. While we understand that DOD may believe that a contractor not receiving or producing covered defense information is already free from the 7012 requirements and that, in such a case, the clause is “self-deleting”, we believe that it is important to make this crystal clear in light of the sensitive nature of the information involved.

Thank you for your consideration of these comments. We appreciate the opportunity to comment.

Sincerely,



Anthony P. DeCrappeo
President
Council on Governmental Relations



Tobin L. Smith
Vice President for Policy
Association of American Universities