

October 30, 2015

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-D018

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 have two principal concerns about the interim DFARS rule:

1. The substantial compliance burdens incurred by our member institutions who handle controlled defense information and will be subject to the new safeguarding and reporting requirements; and
2. The lack of a clear exemption for DOD-funded fundamental research.

Most of our member institutions receive significant research funding from DOD either as direct contractors or as subcontractors. We appreciate the importance of providing appropriate information security for DOD information stored on or transiting contractor information systems. We also appreciate DOD's need to gain greater awareness of the scope of cyber incidents committed against defense contractors. It should be noted, however, that many of our institutions perform only DOD-funded fundamental research, and have not been subject to the previous DFARS 252.204—7012 (Nov. 2013) requirements for safeguarding unclassified controlled technical information (CTI).

We are concerned that the new requirements of the subject interim rule will impose a significant new burden on our institutions that handle CTI or other types of covered defense information under the new 7012 clause. We believe the burden estimate of four hours per response may be several orders of magnitude below the actual burden resulting from the requirements. We are unable at this time to estimate the cumulative impact on our member institutions. However, we can provide some examples. Two COGR member institutions recently received the DFARS 252.204-7012 (AUG 2015) clause. As is true of many universities, their IT systems are not

compliant with the NIST SP 800-171 security requirements specified in the clause. One institution estimates that over a three week period, five staff and the Principal Investigator spent approximately 80 hours trying to find a resolution. The other member institution indicates that to comply, they are considering development of a scalable agile thin-client solution, which is estimated to require one time equipment costs of \$100-\$150K (renewed every five years). Additionally, the ongoing labor costs for three FTE IT personnel, plus software costs to automate some of the processes will cost between \$300,000 and \$350,000.

One of our other members, a public university with a substantial number of DOD contracts, conservatively estimates that the new safeguarding requirements will necessitate a one-time \$1 million hardware/software investment with ongoing maintenance costs of \$200,000 annually. Another of our members, a public institution in the Midwest, estimates that related compliance costs potentially could exceed \$10 million. These examples suggest that the burden of the new requirements will far exceed the cost estimates in the subject DFARS case.

When the NIST SP 800-171 requirements were first proposed, in our comments to NIST we expressed the view that the draft standards would create additional work for universities that use other than NIST standards as their security framework. Additionally, we expressed concerns about the need to formalize campus information security risk management/assessment practices to meet the requirements. We also noted that some of the controls may be very challenging to implement for large decentralized universities. NIST SP 800-171 sets forth 14 “families” of security requirements with over 100 listed controls derived from requirements from multiple publications (e.g. FIPS 199 and 200, NIST 800-53). This number is rather staggering, especially since the previous (Nov. 2013) version of the 7012 clause had only 51 active controls.

As we noted in our previous comments to NIST, a specific example of added burden is the derived security requirement in 800-171 3.5.3 for use of multifactor authentication for local and network access to privileged and non-privileged accounts. Requiring multifactor authentication for network access to non-privileged accounts will be an organizational cost overhead where two-factor authentication is achieved usually by using tokens. For researchers who have non-privileged accounts the number of tokens and the infrastructure to maintain the cost of such hardware will be burdensome for the organization and add costs to the project. Another of our member institutions noted that managing encryption for every laptop and cellphone for any researcher who may have CTI would be “monstrously burdensome” without some mobile device management (MDM) solution in place. This alone would require at least one FTE and a substantial number of vendor licenses.

Our basic concern was that the 800-171 requirements would become compliance requirements without a strong emphasis on the need for flexibility in their interpretation. We urged NIST to strengthen its recognition that non-federal organizations may implement alternate security measures to satisfy particular requirements. The interim DFARS rule confirms our fears. While it contains a provision that alternative but equally effective security measures may be used, it requires that the equivalent measures be approved in writing by an authorized representative of the DOD CIO prior to contract award (252.204-7008). We are not sure on what basis the CIO will make this determination or what information will be deemed sufficient to compensate for the inability to satisfy a particular requirement. Moreover, the timing for this determination and the effect on contract award is not clear.

We observe that the two statutory provisions cited in the DFARS Case (Sec. 941 of the FY 2013 NADA and Section 1632 of the 2015 NADA) apply only to cleared defense contractors and operationally critical contractors. They do not provide a clear mandate for DOD to extend the reporting requirements to all contracts or to require that all contractors report “potentially” adverse effects (the Section 632 statutory requirement containing this language applies only to operationally critical contractors). The “potentially” adverse effects provision greatly increases the number of required reports.

We understand that a pending FAR rule will clarify the marking requirements for controlled unclassified information and provide a taxonomy for identifying such information. Hopefully, it also will provide for self-certification. However, in the meantime, our member institutions that receive the DFARS clauses will incur substantial compliance costs in redesigning their business systems to comply with what may only be *interim* requirements. It appears premature for DOD to impose these requirements in advance of the government-wide implementation, especially given the lack of a clear statutory mandate. We urge DOD to reconsider the imposition of these requirements on contractors beyond what is required by the NADA.

We also are concerned that the 7012 definition of *Export Control* information in subset (C) of *Covered Defense Information* expands the scope of this information beyond the authorized scope. The language defining export controlled information (7012(a)(C)) as “unclassified information...whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives” has no basis in the current export control regulations. This subset should be limited to technologies subject to the EAR or ITAR or sensitive nuclear technology subject to the nuclear export regulations, and related license applications. DOD has no authority to expand the definition of export controlled information beyond this scope. Similar concerns also arise over the “any other information... identified in the contract that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations and Government wide practices ...” in (D) of this subsection. This conceivably could subsume a wide set of regulations for which DOD has no responsibility (e.g. health, student information).

With the interim rule it becomes even more critical to ensure that our member institutions who solely conduct fundamental research with DOD funding do not become inadvertently subject to the new requirements. Previous acceptance of controls on disclosure of information pursuant to the DFARS 252.204-7000 clause would result in all project information becoming controlled technical information (CTI) subject to the previous 7012 requirements. With the expansion of the 7012 clause to include “covered defense information” (of which CTI is a subset), it becomes even more important to ensure that fundamental research remains exempt.

The process that we previously worked out with DOD to obtain fundamental research determinations under 7000(a)(3) and the related PGI 202.403—70 should continue to apply. Moreover, we suggest that the policy guidance in DFARS 204.7302 include a new provision (f) that references projects determined to be fundamental research pursuant to 7000(a)(3) as not involving covered defense information subject to the safeguarding requirements. A similar statement would be beneficial in clause 252.204—7008. We are concerned that without an explicit reference, there may be a tendency for DOD contracting officers to apply the new 7012 requirements even when the project is fundamental research. We request that the final rule reaffirm the fundamental research exemption and reiterate this in the DOD PGI. This is especially important given that the 7012 requirements flow down to subcontractors.

We understand the new DFARS Subpart 239.76 on cloud computing applies to acquisition by DOD of commercial cloud computing services. We assume that the new clauses 252.239—7009 and 7010 apply only in these situations. Our member institutions are not cloud computing service providers, and normally should not be subject to these clauses. We are concerned that these clauses may be read as applying to any use of cloud computing under a DOD contract. Requirements such as compliance with the Cloud Computing Security Requirements Guide (7010(b)(2)) or maintaining data within the U.S. (7001(b)(3)) are onerous, and compliance may not even be possible. It has been the experience of our member institutions that most cloud providers insist on storing data anywhere they want to. Thus, we urge DOD to include clarification that contracts for fundamental research or other services where use of cloud computing is incidental to contract performance are not subject to the requirements of 239-7600 and related clauses.

The accretion of unfunded compliance requirements such as those in the subject interim rule are of increasing concern, and have been the subject of a number of recent reports. DOD needs to acknowledge and recognize the cost implications in solicitations and contracts that require use of the 7012 clause, and provide funding to defray the related costs. Otherwise universities and other contractors such as small business may be unable to meet the requirements. FAR 52-204-2 recognizes the need for the government to provide an equitable adjustment in contract costs when security requirements are changed by the government (and also provides an alternate clause for research and development contracts with educational institutions for changes in security requirements). As not-for-profit institutions, universities are unable to build these costs into approved contract fees, and can only recover these costs through periodic renegotiations of facilities and (capped) administrative (F&A) costs. Researchers may be driven to use outside servers, in which case the related costs should be explicitly recognized in project budgets. In extreme cases, they or their institutions may determine that the costs and burdens of compliance are too high to perform work for DOD or other federal agencies that impose similar IT security requirements. We do not believe this is in any of our interests.

We note that on October 2, 2015, DOD issued an interim rule revising its cybersecurity regulation to mandate reporting of cyber incidents that result in an actual or potentially adverse effect on a covered contractor information system or covered defense information residing therein, or on a contractor's ability to provide operationally critical support (80FR59581). The rule is inappropriately and unnecessarily broader than the subject DFARS rule. In addition to all forms of contracts (including research contracts), the scope includes cooperative agreements and other transactions involving covered defense information.

The relationship between this rule and the DFARS rule is not clear. The cyber incident reporting requirements implement the same section (Section 941) of the FY 2013 National Defense Authorization Act. The reporting requirements appear identical and redundant to the DFARS. We urge DOD to clarify the relationship between these two interim rules. The concerns we have stated thus far about the DFARS rule, may also apply to this rule.

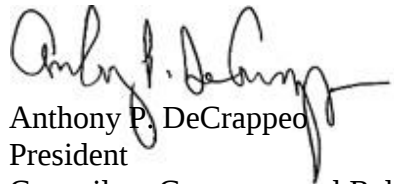
In addition, the new cybersecurity regulation recognizes that contractors will incur costs associated with the requirements, including identifying and analyzing cyber incidents and their impacts and obtaining the medium assurance certificates. It does not say DOD will pay these costs. This reinforces the discussion above about the need for DOD to provide funding for the

added compliance costs in contracts and other awards involving covered defense information subject to the cybersecurity requirements.

Our member institutions, COGR and AAU value our long and productive working relationship with DOD. All of our member institutions have established information security requirements and are very familiar with the need to protect information system infrastructure and processes. We also are very aware of the increasing cyber threats facing both the government and our institutions. However, we also need to be assured by the government that there will be balance and flexibility in the application of new security requirements. Government imposition of stringent security controls on unclassified information raises serious policy issues. Therefore, we strongly urge DOD and the Office of Management and Budget to recognize the burden and cost implications of the new requirements and to provide assurance that they are not applied inappropriately. Fundamental research should continue to be clearly exempt.

We appreciate the opportunity to comment.

Sincerely,



Anthony P. DeCrappeo
President
Council on Governmental Relations



Hunter R. Rawlings III
President
Association of American Universities

cc: John Holdren, Director, White House Office of Science and Technology Policy
Steve Fetter, Principal Assistant Director for National Security and International Affairs,
White House Office of Science and Technology Policy
Howard Shelanski, Administrator, Office of Information and Regulatory Affairs, Office
of Management and Budget
Jasmeet Seehra, Desk Officer for Department of Defense, Office of Management and
Budget
Robin Staffin, Director for Basic Research, Department of Defense