



David Brady, Chair  
2000 Kraft Drive, Suite 2000 (0497)  
Blacksburg, Virginia 24060  
540/231-3801 Fax: 540/231-0959  
E-mail: [dbrady@vt.edu](mailto:dbrady@vt.edu)

April 30, 2010

Defense Acquisition Regulations System  
Attn: Mr. Julian Thrash  
OUSD (AT&L) DPAP (DARS)  
3060 Defense Pentagon, Room 3B855  
Washington, D.C. 20301-3060

**RE: Defense Federal Acquisition Regulation Supplement; Safeguarding Unclassified Information (DFARS Case 2008-D028)**

To Whom It May Concern:

I am writing on behalf of the Association of University Export Control Officers (AUECO), an association of senior export practitioners with export compliance responsibilities at sixteen accredited institutions of higher learning in the United States. As expressed in its founding charter, AUECO is committed to monitoring changes in the administration of export laws and regulations that could affect international transactions and collaborations in academia. As a result, AUECO is providing the following comments in response to the Department of Defense (DoD) advance notice of proposed rulemaking on potential changes to the Defense Federal Acquisition Regulation Supplement (DFARS) to address requirements for the safeguarding of unclassified information.

While AUECO does not believe that it is DoD's intent to do so, the practical effect of the adoption of this proposed rule will be to eliminate DoD contracted fundamental research. As expressed through National Security Decision Directive 189, it has been executive policy since 1985 to prohibit restrictions "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." Of particular concern is the inclusion of information "used in support of an official DoD activity" within the definition of "DoD information". This statement effectively turns any institutional information obtained under other funding that is used in connection with or in support of a DoD contract into "DoD information". This proposed change would restrict our ability to use our own information for academic purposes or to fulfill our obligation to a non-DoD sponsor's requirement that we publicly disseminate research findings.

**Statutory Authority**

The definition of DoD Information in the proposed rule is an excellent example of why the President's Task Force on Controlled Unclassified Information (CUI) recently recommended a moratorium on new regimes of CUI until a government-wide framework is implemented. As defined in the proposed rule DoD Information appears to impact a relatively small subset of CUI, but there are actually 107 unclassified control regimes and at least 117 different CUI markings that potentially trigger the application of the proposed DFAR 252.204-7000 clause (see Appendix 2 of the President's Task Force

Report and Recommendations). Pursuant to the proposed rule, "access to or generation of" any information "[b]earing current and prior designations indicating controlled access and dissemination (e.g., For Official Use Only, Sensitive But Unclassified, Limited Distribution, Proprietary, Originator Controlled, Law Enforcement Sensitive)" would mandate the inclusion of the DFAR 252.204-7000 clause, restricting disclosure of any unclassified information about the contract without DoD approval. However, the statutory authorization of DoD to control much of this information is unclear.

AUECO cannot determine from the ANPR, or from the information presented in the 22 April 2010 public meeting, what laws, executive orders or regulations DoD is attempting to implement in this regulation. We ask that DoD clearly cite the authority(ies) under which it establishes control over each category of controlled unclassified information, and by extension authority to expand control to all unclassified information utilized in the conduct of a DoD contract. "If the official status determination of the level of access and dissemination of the information cannot be determined, the information will be considered DoD information until the official status can be ascertained from the cognizant DoD activity" is insufficient reasoning and constitutes far too broad a reach.

The ANPR includes proposed changes that would add requirements for control of information under the jurisdiction of other agencies (e.g. export controlled information under the jurisdiction of the Departments of State and Commerce) or information that already has a statutory requirement for protection, for example the Health Insurance Portability and Accountability Act (HIPAA). Including information subject to other requirements would create burdensome duplicative controls. Does authority for this reside in the Federal Information Security Management Act, the Computer Security Act (FISMA), or some other authorization? If FISMA, the proposed rule would appear to far exceed the authority delegated to DoD in the act. If the Computer Security Act, the scope of that Act is limited to only government computers and expressly prohibits control over privately held computers or privately owned information.

Also, inclusion of information "Subject to export controls under International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR)" as DoD Information in 204.7XX2(d)(2)(ii) and 252.204-7YYY(b)(2)(ii) is problematic. DoD has no legal authority to promulgate regulations governing the release of export-controlled technical data under the jurisdiction of the Department of State or the Department of Commerce. Specifically, by requiring Contracting Officer approval for release of export-controlled technical data, when the ITAR or EAR permits its release or export pursuant to a license or exemption, DoD has usurped the regulatory authority of the cognizant regulatory agency in violation of the limits placed on DoD authority in 10 USC 130. Moreover, an obligation will be placed on the Contracting Officer to determine whether or not the unclassified information proposed for release is export-controlled. In its final rule on export compliance in contracts (75 FR 18031) issued 8 April 2010, DoD declined this role, stating: "Additionally, authorization to release and for releasing export-controlled items is covered by export control laws and regulations and is, therefore, independent of, and beyond the scope of, this DFARS rule."

Finally, AUECO does not understand why the regime chosen for this proposed rule is located in a subpart designed for classified materials (Subpart 204.4 refers to SAFEGUARDING CLASSIFIED INFORMATION WITHIN INDUSTRY). The Subpart applies to DoD employees or members of the Armed Forces who are assigned to or visiting a contractor facility and are engaged in oversight of acquisition programs (204.404). This subpart does not appear applicable to research contracts conducted at institutions of higher education, which are not considered "industry" under the FAR, just as research and development

contracts which are not considered acquisition contracts under the FAR. Much has changed since the clause at DFAR 252.204-7000 was amended to its current form in 1991. If the intent of DoD is to have this clause apply to research and development contracts at colleges and universities as well as acquisition contracts in industry, the policy section should be amended to provide guidance to Program Managers and Contracting Officers about the differences in applying the clause in each type of contract, and to not apply the clause in contracts involving institutions of higher education conducting fundamental research in accordance with the DoD Policy on Contracted Fundamental Research dated 26 June 2008. This policy prohibits DoD restriction on basic research in either industry or academic institutions, and places extraordinarily strict limits on DoD controls on any applied research at institutions of higher learning. AUECO believes that implementing such a policy section, in addition to other recommendations in this letter regarding necessary changes to the prescription and clause, may go far to alleviate the concerns we have addressed that all DoD contracts are likely to be subject to this clause under the proposed rule, effectively ending DoD contracted fundamental research.

### **Deficiencies in the Prescription for the Disclosure of Information and Fundamental Research**

The prescription for the fundamental research clause needs to be amended as it does not mandate that the Requiring Activity inform the Contracting Officer when a given contract should be considered Fundamental Research. In its final rule on export control clauses (75FR18030) issued 8 April 2010, DoD removed both the definition of fundamental research (204.7301) and the prescription clause for fundamental research (204.7304) directing the requiring agency to notify the contracting officer in writing when "the work is fundamental research only, and export-controlled items are not expected to be involved." Absent these clauses or a functional equivalent, how is the contracting officer to know when the scope of work is fundamental research? At the very least, the DoD Policy Memorandum on Contracted Fundamental Research should be referenced when contracting with universities.

Clause 204.7XX3 introduces a concept called a "validated requirement" for DoD Information. What is this and who is conducting the validation? Will the requiring agency provide this validated requirement to the contracting officer in writing, and through what contracting mechanism or prescription? In the absence of a validated requirement, what clauses should the contracting officer include concerning DoD information, if any?

### **Conflict between 204.7XX3 and 252.204-7000(c) in Subcontracts**

In cases where a Contractor issues a subcontract, pursuant to the clause at DFAR 252.204-7000 (c) "The Contractor agrees to include a similar requirement in each subcontract under this contract." This generally means flow down of the clause DFAR 252.204-7000 to the Subcontractor. However, in accordance with 204.7XX3(a)(1), the clause should not be included unless "...the contractor will have access to or generate DoD information." This is especially problematic when the Subcontractor is a university. In this case, even though the university may be conducting contracted fundamental research per the DoD Policy Memorandum "Contracted Fundamental Research" dated 26 June 2008, and will not require access to or generate DoD Information and should not be subject to the clause in accordance with 204.7XX3(a)(2), the Contracting Officer for the Prime Contract has conflicting guidance on how to proceed. The clause at 252.204-7000 must be amended to allow the Contracting Officer to exclude the clause for subcontracts meeting the criteria of (a)(1). In conjunction with necessary narrowing of the scope of "DoD Information", and modification of the prescription, this circumstance might be mitigated by the following change to 252.204-7000(c):

c) Except as prescribed in 204.7XX3(a)(1), the Contractor agrees to include a similar requirement in each subcontract under this contract. Subcontractors shall submit requests for authorization to release through the prime contractor to the Contracting Officer.

### **Definition of DoD Information**

As proposed, "DoD information" means any unclassified information that has not been cleared for public release in accordance with DoD Directive 5230.09, Clearance of DoD Information for Public Release, and that is "(1) Provided by or on behalf of DoD to the contractor or its subcontractor(s); or (2) Collected, developed, received, transmitted, used, or stored by the contractor or its subcontractor(s) in support of an official DoD activity." What constitutes "an official DoD activity"? Likewise, what is meant by the phrase "conducted in support of an official DoD activity"? Would the DoD contract or subcontract in and of itself be sufficient to warrant designation of the research as an official DoD activity? If this is the case, then theoretically all contracts would involve DoD Information and thus all contracts would require the 204-7000 clause. Without a formal definition it will be impossible for Contracting Officers to determine what activities might be considered to be "conducted in support of" the DoD activity.

The definition of DoD Information when taken together with the prescription for inclusion of the 204-7000 clause, as proposed, will result in its inclusion in all DoD contracts not definitively predetermined to be fundamental research (i.e., had other than Distribution A on the DD1423). In cases in which DoD Information will be accessed or generated as part of a research project, then the 204-7000 clause would be immediately applied to the contract, eliminating the fundamental aspect of the research. Many universities cannot accept projects that impose publication restrictions, so the result of broad application of the 204-7000 clause will be to preclude many universities from participating in DoD-funded activities.

Although the proposed definition of DoD Information appears to relate solely to securing government information, the definition is misleading. For all practical purposes, "DoD Information" will also include any "contractor unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of any DoD contract or any program related to such contract." If the Contractor has access to or generates any information identified with the access or dissemination controls (including its own contractor proprietary information in accordance with 204.7XX2(d)(iv)), it becomes DoD information. Once DoD information is identified, the Contracting Officer would then apply the clause at 204-7000 and all unclassified contractor information relating to the clause becomes "controlled unclassified information" requiring Contracting Officer's written authorization to release. Such application of 204-7000 would add considerable burden on academic fundamental research, if not eliminate it altogether with regards to work performed under contract from DoD. For example, contracts to assess environmental performance would typically require the collection and use of significant amounts of information regarding environmental parameters. By the proposed definition, this environmental data would be considered DoD information regardless of when, how, by whom, and under what funding the information was collected. Such data is often collected under federal funding from non-DoD agencies that require its dissemination and use. Similarly, the proposed definition does not specifically exempt data already in the public domain.

The proposed text of 252.204-7YYY(b)(2) enlarges the scope of "DoD information" even further by essentially identifying all controlled unclassified information (CUI) as "DoD information requiring enhanced safeguarding". It is likely that this will lead contracting officers to apply the DFAR 252.204-7000 clause to any work involving access to or generation of any CUI or even potential access to or generation of CUI (see 204.7XX3(b)(1)). This will have multiple negative effects on university research. First, the presence of the DFAR 252.204-7000 clause is a publication restriction, the inclusion of which destroys the ability of the university to conduct research as fundamental research, not subject to export control regulation. Second, the presence of a publication restriction will jeopardize researchers' ability to publish, and students' ability to graduate as publication of their dissertation or thesis would require government approval. As an example, 252.207-7YYY(b)(2)(vi) specifically includes personally identifiable information protected pursuant to HIPAA; therefore, any DoD project funding basic medical research will be determined to include "DoD information" and the contracting officer will include the DFAR 252.204-7000 clause eliminating the ability to conduct the research as fundamental.

The preceding examples are only two of innumerable examples where the contractor would be required to protect information the release of which would pose no, or by even the most conservative standards very minimal, risk to national security. As we see this issue, there is no need to restrict publication in order to secure cyber information. NIST standards are applied by NIH without restricting publications. DoD should be able to achieve the same result without restricting publications (through application of the DFAR 252.204-7000 clause) and adding additional burdens on both sides of the contracting process.

#### **Safeguarding Guidance Unclear**

Guidance concerning how safeguarding will be managed is not clear under the proposed rule. Many questions still remain, such as: Will security plans be subject to review to determine adequacy and prior approval? If so, will the review be conducted by the Prime Contractor, Contracting Officer, Requiring Agency, or some other entity? Will approval, if required, be recognized across all DoD activities or will independent reviews be required for each contract/subcontract or for each contracting agency? What are the penalties for failure to "adequately" protect DoD information? The reporting requirement in 252.204-7YYY(c) Cyber intrusion reporting, appears to violate our right not to self incriminate. The ITAR and EAR both suggest voluntary reporting and will consider it a mitigating factor in the assessment of penalties, but do not require self incrimination in this way. It is unclear whether or not the reporting requirement applies to "door-knocks", actual intrusions where there is perceived loss or compromise of equipment or data, or both. A major university might receive millions of door knocks a year, and it would be extraordinarily difficult to report (and for DoD to meaningfully process) such intrusion information, if required. It is unclear what is meant by "best practice"; the only way to completely secure this type of information would be to close it off from network connectivity. If that is to be a standard, then it needs statutory authorization, rather than implementation as a contractual clause.

Why is it necessary to include information subject to the EAR, ITAR, HIPAA, etc. as protected "DoD information" requiring "enhanced safeguarding"? Any proposed requirements for safeguarding information subject to the jurisdiction of existing regulations should come from the cognizant agency(ies).

## Administrative Burden and Unallowable Costs

The basic safeguarding requirement 252.204-7XXX(b)(3) requires that electronic information be transmitted "using technology and processes that provide the best level of security and privacy available, given facilities, conditions, and environment." The use of the term "best" is overly vague and therefore burdensome. The requirement that contractors use state of the art technology and processes could potentially subject colleges and universities to significant additional costs associated with continually upgrading systems and processes.

Similarly, 252.204-7XXX(b)(7) requires contractors to "provide protection against intrusions and data exfiltration, minimally including the following: (i) Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware, (ii) Prompt application of security relevant software upgrades, e.g., patches, service-packs, and hot fixes". The use of "e.g." implies that there are other required protection services and software upgrades that are not listed. This puts an unnecessary burden on contractors to determine additional requirements. Likewise, the terms "regularly" and "prompt" are imprecise and will lead to inconsistent application. Dealing with these requirements will be especially difficult for large and diffuse organization like many universities which may have a decentralized IT structure.

The definition of "adequate security" requires the performance of a risk assessment. Who will bear the burden and liability for performing the risk assessment? In many situations the contractor or subcontractor(s) may not be provided with the necessary information to be able to perform an accurate risk assessment. If an official status determination is sought from the cognizant DoD activity, as allowed in 252.204-7XXX(b)(1), in what timeframe will the agency be required to provide its determination to the contractor?

Although 252.204-7YY(c)(1) specifically states that only intrusion events that affect DoD information must be reported, section (c)(2)(iii) broadens the scope to include any intrusion activities that "allow illegitimate access to an unclassified information system on which DoD information is resident or transiting. This clause necessitates reporting unauthorized system access even when there is no evidence that DoD information has been accessed or compromised and will impose a significant compliance burden on the contractor's IT systems and personnel, with inherent associated monetary costs.

The area that may be most lacking is the enhanced requirement referring to a security program and NIST 803-53. Most large research institutions have an enterprise-wide security program in place. The framework would probably suffice in most areas given the "as appropriate" wording. However a costly risk assessment will be needed to determine the appropriateness of a standing system.

Enhanced requirements Section 204.7YYY(b)(3)(i) is poorly worded. We believe the intent is to require that wireless communications be encrypted and that data should be encrypted when transmitted over an unencrypted wireless link. However, the wording suggests that an encrypted wireless connection is preferred to a wired connection, encrypted or not. This section also requires that all mobile devices storing the indicated data be encrypted using the "best technology available given facilities, conditions, and environment". There is no definition of "best." We would argue that it should be equivalent to "as appropriate." However, an ensuing risk assessment would be needed for each contract to determine adequacy; this could necessitate costly improvements that would be unallowable as direct costs.

## ORCA Certification

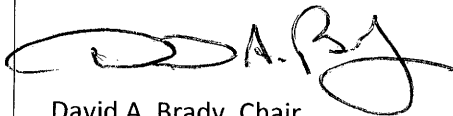
The Online Representations and Certifications Application (ORCA) allows for a broad base sweep of contract clauses, many of which are acceptable to universities and other contractors regardless of the instant contract being proposed. 252.204-7000 and the proposed additions at 7XXX and 7YYY should only be applied on a contract-specific basis.

## Closing

Even though we believe this is not the intent of DoD, adoption of this proposed rule will have the practical effect of eliminating DoD contracted fundamental research. National Security Decision Directive 189 and executive policy since 1985 prohibit restrictions "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." The language in this proposed rule will result in Contracting Officers applying DFAR 252.204-7000 to university contracts thereby restricting our ability to use information for academic purposes and to fulfill our obligations to non-DoD agencies.

In closing, AUECO would like to express its appreciation for the opportunity to provide comments on these proposed changes.

Sincerely,

A handwritten signature in black ink, appearing to read "D.A. Brady", with a stylized flourish at the end.

David A. Brady, Chair  
Association of University Export Control Officers