AUECO
ASSOCIATION OF UNIVERSITY EXPORT CONTROL OFFICERS

December 15, 2011

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

RE: DFARS Case 2011-D039
Submitted via: Regulations.gov or dfars@osd.mil

To Whom It May Concern,

I am writing on behalf of the Association of University Export Control Officers (AUECO), a group of senior export practitioners at 22 accredited institutions of higher learning in the United States. AUECO members monitor proposed changes in laws and regulations affecting academic activities and advocate reforms that will improve the efficiency and effectiveness of the United States export control system. AUECO is specifically interested in contributing to the export control reform effort in order to ensure that the resulting regulations do not have an adverse impact on academic pursuits. As a result, AUECO is providing the following comments in response to the Department of Defense (DoD) Defense Federal Acquisition Regulations Supplement's (DFARS) proposed clauses on Safeguarding Unclassified DoD Information (DFARS Case 2011-D039).

AUECO recognizes and appreciates the need to safeguard DoD Information in the possession of contractors and subcontractors. However, we are concerned with the breadth of the proposed clauses, particularly the clause entitled "Enhanced Safeguarding", and the burden this regulation will have on the regulated community. As will be further described below, we believe the clauses are generally too broad – thereby diminishing the practical utility of the clauses – and need clearer definitions of the Department's expectations for the regulated community. Contract clauses should not be vague as such construction invariably leads to differing interpretations and could result in misunderstanding and dispute. Given the subject matter at issue, the risk is too high to leave such clauses open to arbitrary interpretation. We ask the Department to review the proposed language to ensure consistent interpretation and application in contractual agreements.

Cyber Incident Reporting – Burden on the Regulated Community

In a number of ways, the cyber-incident reporting requirement involving possible data exfiltration, manipulation, loss or compromise of unclassified information is more stringent than the National Industry Security Program Operating Manual (NISPOM) reporting requirement for loss, compromise, or suspected compromise of classified information. Whereas the proposed rule requires cyber-incident reporting within 72 hours of discovery, the NISPOM does not specify a fixed time requirement for the initial report of loss, compromise, or suspected compromise of classified materials (NISPOM 1-304).

Further, the proposed rule at 252.204-70YY(f)(2)(ii) requires cyber-incident reporting even in instances in which the Contractor can positively determine that a cyber-intrusion did not involve unauthorized access to DoD Information. Under the NISPOM, if the Contractor has positively determined that no loss or compromise occurred, no such reporting is required (NISPOM 1-303).

The proposed clause references a specific DoD form to be used in reporting intrusions and exfiltration, but the form has not been provided for review and comment. The form in question, "Contents of Cyber incident report" at 252.204-70YY(f)(4), is the basis of the report which will fulfill the 72 hour notification requirement. A request for the anticipated contents of the report was made by AUECO on 2 August 2011. The response indicated that the reporting fields would not be provided until publication of the final rule. Without the opportunity to review the report form and its contents, it is impossible to respond to the potential burden such a report may have on the regulated community. The Department should produce the report and allow for comment before any final rule is proposed.

Further, some of our members have been involved in investigations akin to the ones anticipated in this section. In one instance of a limited cyber-intrusion, the forensic investigation alone took upward of 100 man-hours to complete. If the 72-hour report requires such specific information, it is unlikely that an entire information technology workforce focused on the investigation from the moment it occurred could possibly create the report in the time frame mandated by the clause. A more reasonable option would be to adopt an initial/final report format similar to the NISPOM's initial/final report, or the voluntary disclosure process of International Traffic in Arms Regulations (ITAR) (i.e. initial report that outlines what is known at the time with a final report to follow within 60 days).

252.204-7000 Disclosure of Information.

AUECO is concerned with the definition of "DoD Information". We understand that the clause requires "technical data, statements of work or other information subject to Distribution Statements" receive enhanced safeguarding. However the definition is overbroad. For example, Distribution A is subject to DoD Directives 5230.24 and 5230.25, and therefore defined in clause 70YY (b)(6) as DoD information. However, Distribution Statement A indicates that a document is approved for public release and eligible for unlimited distribution, and should be outside of the scope of the clause. We request that the Department include a specific carve out for Distribution Statement A to avoid confusion.

Further, we feel that unclassified nonpublic information "provided by or on behalf of the DoD to the contractor or it's subcontractor(s); or, collected, developed, received, transmitted, used or stored by the Contractor or its subcontractors in support of an official DoD activity" is far too broad a scope for this definition. It makes sense that the research activities defined in a scope of work conducted under a DoD contract could be interpreted as an "official DoD activity", but it is unclear that this is the intent. We ask the Department to define specifically the parameters of "an official DoD activity." Protection requirements for third party information provided to a contractor in support of a DoD activity are typically imposed via a non-disclosure agreement (NDA) or similar contract clause. Addition of a separate DoD requirement is unnecessary and may create conflicting requirements and expectations. If the information is the product of a prior DoD activity then that should be specified by the provider in the NDA with reference to the control requirements.

The proposed revision to the 252.204-7000 clause specifies that DoD information is non-public information that has not been cleared for public release in accordance with DoD Directive 5230.09. As this directive specifically states that it does not apply for provisions governing review of information

before publication or disclosure by DoD contractors, it is unclear from the clause whether new information generated by a contractor under a DoD contract would be DoD information and subject to the 'safeguarding DoD Information' clauses. Clarification on this point is essential.

Section (b) of the clause proposes that the Contractor shall not release unclassified DoD information pertaining to the contract or any program related to the contract. Much like the definition of DoD Information, we feel this is an extremely broad statement that lacks specificity. Additionally, this section restricts information dissemination to only those employees with a "need to know" – a concept exclusively associated with regulations for the control of classified information. Expanding that concept to include unclassified information would result in the need for an entire staff of personnel to review all information "related to the contract", determine who "needs to know", and monitor for any changes to such status.

This requirement would also prohibit the contractor from obtaining outside expert consultation absent a formal subcontract, which could impede progress for example in cases where consultation is required to adapt a procured item to meet the specific needs of the DoD activity. Even within the Contractor's organization, the need to know requirement will chill collaborative activities among researchers. It will create internal program silos, in which the research results cannot be shared with peers absent a formal determination of who has a "need to know", and to what information that "need to know" extends. Such a system is antithetical to the university research model in which the broadest review of results as possible is sought to critique existing results and bring in new ideas and approaches into the research.

Requiring standards of control for unclassified information- the release of which will not cause national security damage-that meets or exceeds that for classified information is unprecedented and unreasonable. The "need to know" requirement should be eliminated or better defined to relieve the unreasonable burden its inclusion in this section would undoubtedly cause.

AUECO also feels that the section describing the certification process for information that "results from or arises during performance of fundamental research", needs further clarification. The clause proposes that the project be scoped, negotiated, and determined to be fundamental research within definition of National Security Decision Directive (NSDD) 189. When universities are involved, whether as the prime or a subcontractor, the negotiation and determination of whether fundamental research is being performed needs to occur at the proposal stage. It is critical for the university to know if the Department concurs with the fundamental research determination prior to award as later disagreements could significantly delay progress and may result in the university having to withdraw if the proposed scope is determined to be something other than fundamental research. Our members also find that often companies are unwilling to go back to the Department for fundamental research terms on existing contracts when they decide to add a university subcontractor later. This is particularly true for relatively small (both in terms of scope and monetary award) subcontracts and when the prime contract is awarded to a small to medium sized business, especially ones new to DoD contracting. Companies may agree that the university's scope is fundamental, but are unwilling to ask the Department for the correct DFARS terms.
Also, the clause requires that the determination must be conducted by both the prime contractor and research performer. At an academic institution, the "prime" could be interpreted as the institution itself, while the "research performer" could be the faculty member investigator, a subcontractor, or some combination of the two. The contracting component certifying the fundamental research aspect could be either the prime's contracting office or the DoD Contracting Officer. To ensure appropriate processing of such requests, AUECO would like clarification of who exactly the Department wants

involved in this process. Our own members have varying interpretations of this aspect of the clauses and therefore we feel it would assist the entire academic community to have a clear understanding of this requirement. Significant outreach is needed to DoD primes, particularly small to medium sized businesses that are new to DoD contracting who will be subcontracting to universities, to ensure they understand what constitutes fundamental research and that specific contracting terms are available that should be used in these instances.

252.204-70XX Basic Safeguarding of Unclassified DoD Information.

The proposed clause at 252.204-70XX Basic Safeguarding of Unclassified DoD Information addresses protection for unclassified "Government Information." We understand the goal to prevent the unauthorized disclosure, loss or exfiltration, and can support expectations presented in this section; however, we reiterate our concern expressed above about the definition of "DoD Information" and also ask the Department to clarify the distinction between "DoD Information" and "Government Information." The Government Information definition contains the same broad language present in the proposed definition of "DoD Information" and the same problems inure with its structure. We ask the Department to specifically define "official Government activity" and further indicate the differentiation as compared to an "official DoD activity."

AUECO would like to express concern with the definition of "Compromise". The definition captures "disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred." We feel the use of "may" causes this definition to echo the restrictions on disclosure found in the NISPOM, particularly Chapter 4 Section 218 and Appendix C-1. As with the proposed "need to know" requirement, applying terms of art found in the NISPOM to unclassified information is overly burdensome and unreasonable. Similarly, the fact that cyber-intrusion reports must be filed regardless of whether DoD information is actually accessed, exfiltrated, or otherwise impacted is likely to result in a large burden on the Department to review and analyze events that are in fact false positives where no breach has actually occurred.
AUECO is particularly concerned with the broad, ambiguous language in the safeguarding requirements of this proposed clause. The clause contemplates providing 'adequate security', but seems to leave that determination of what constitutes adequate security up to the contractor. We are concerned this would allow too much disparity among contractors' baseline systems and could result in an enforcement action if the Department feels the contractor-determined baseline was not sufficient. It is also likely to lead to prime contractors placing additional controls on subcontractors that may or may not be warranted based on an objective risk assessment. We ask the Department to clearly state the expected baseline. Also, the same concern is reflected in subsection (2) "Transmitting electronic information", in that the Contractor is expected to "provide the best level of security and privacy available, given facilities, conditions and environment." We feel this is very subjective and demands a more concrete expectation. We believe providing the expected baseline will give additional clarity at the contract clause level and will ultimately provide better protections and enhanced compliance within the regulated community.
252.204-70YY Enhanced Safeguarding of Unclassified DoD Information.

The proposed clause at 252.204-70YY Enhanced Safeguarding of Unclassified DoD Information requires creation of an elaborate control platform for data storage and transmission, network protection, intrusion detection and cyber intrusion reporting. The expectations present in this section will result in a tremendous burden, both to staff oversight and financial support for such systems. The proposed rule asks for specific comments on the impact to small businesses, but the burdens imposed by this clause

will result in an incredible hardship for businesses of any size. This impact will be more profound at universities where information technology infrastructures are designed to support the institution's core educational/not-for-profit mission rather than a business/commercial mission. Such overregulation would have adverse consequences for the continued growth and development of a robust defense research and development industry in the United States, and for the United States' position as a world leader in military technology development. The net effect of these impacts will be to inhibit the development and production of new technology and products. As a result, the U.S. will lose not only the promise of job creation, but also its position as a technological leader.

Putting together an enterprise-wide information security program that is National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 compliant requires a tremendous effort and vast resources. Given that NIST SP 800-53 appears to be the Department's baseline for 'enhanced safeguarding,' due consideration must be paid to the additional staffing and financial burden that such a requirement would impose on a contractor of any size. As a general rule, academic institutions are not-for-profit organizations that are decentralized and perform a wide variety of work. Applying NIST SP 800-53 standards enterprise-wide would be overly burdensome to the vast majority of the work occurring on a college campus and may inhibit the institution's ability to support its core educational mission. While applying NIST SP 800-53 in discrete instances is perhaps more manageable on the surface, the infrastructure to support such an effort on even a small scale is still expensive and would require considerable resources to achieve. The financial burden of applying such a massive information security infrastructure to unclassified information should be seriously considered by the Department. AUECO asks that this proposed burden be fully vetted and before its adoption is determined to be consistent with Executive Orders 12866 and 13563.

We understand that the proposed clause provides the Contractor the option, instead of establishing NIST SP 800-53 security, to prepare a written determination citing its reasons why current security measures are sufficient or why NIST SP 800-53 is not necessary to achieve enhanced safeguarding. However, the Department could very easily disagree with the Contractor after the fact thereby placing the contractor at significant risk. We feel this proposed work-around is far too subjective to be reasonably applied.

As discussed previously, the cyber incident reporting requirement described in section (f) – Contractor shall report to DoD within 72 hours of discovery of any cyber incident … that affects DoD information resident on or transiting through the Contractor's unclassified information systems – is unrealistic. Subsection (f)(2)(ii) requires that essentially any type of intrusion incident is reported which is more stringent than the reporting regulations in the NISPOM for the safeguarding of classified information. What Contractors are being asked to safeguard through application of these clauses is unclassified. Therefore, it is unreasonable to establish a structure that is more stringent for unclassified information (e.g. secrets of far less consequence) than that for classified (e.g. the country's most important secrets). We recommend one of the following options be utilized: 1) employ a staggered NISPOM-like preliminary/initial/final reporting structure (reference: NISPOM Section 1-303 Reports of Loss, Compromise, or Suspected Compromise); or 2) employ the voluntary reporting requirements similar to that found in the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) (references: ITAR Section 127.12; and EAR Section 764.5).

As stated above, the lack of information about the contents of the 72-hour report is of tremendous concern. Additionally, the requirement at (f)(2)(i) to report incidents "involving possible data exfiltration or manipulation or other loss or compromise" is untenable. Through normal auditing and review

processes, our members often find that a "possible" incident was actually a false-positive. Even this determination – as simple as it may sound – regularly takes longer than 72 hours to determine. If DoD information was involved in the false-positive cyber incident, the reporting effort alone would be reduced in value to paper pushing and provide no practical utility to the Department.

Finally, the forensic evidence we are being asked to provide is of major concern. As the proposed clause states at section (f)(5)(iii), "The Contractor shall preserve and protect images of known affected information systems … until DoD has received the image and completes its analysis,…". If, for example, the reported intrusion included Family Educational Rights and Privacy Act (FERPA) information, providing that information to the DoD Damage Assessment Management Office (DAMO) would be prohibited without waivers from all affected individuals. This is further concerning as the proposed clause states in section (h)(i) that the "contractor will seek written permission from the owner of any third-party data...". The FERPA laws, as well as other privacy regulations such as those protecting human subject participants in research, would likely not include provision of such information to DAMO. Re-consenting every student and every research participant to cover releases to DAMO would be overly burdensome and extremely difficult to achieve 100% compliance. Likewise, although non-disclosure agreements and contract clauses typically address the parties obligation to provide information in response to a subpoena or court order those provisions, as currently constructed these clauses would not permit providing proprietary information to DAMO and it would be impractical and unduly burdensome to renegotiate all existing confidentiality agreements to address the possibility of disclosure to DAMO related to an intrusion event.

Conclusion

In closing, AUECO would like to express its appreciation for the opportunity to provide comments on these proposed changes. Safeguarding of unclassified information is an important and inherently complex topic, and AUECO would like to thank the Department for taking the time necessary to consider the impact of the proposed clauses. It is AUECO's position that the proposed clause for Enhanced Safeguarding is unduly burdensome to the regulated community. However, should the Department choose to proceed with the proposed clause as written, AUECO would strongly encourage the Department to clearly define the parameters of the expectations and to consider modifications to significantly reduce the reporting burden.

Sincerely,

Sincerely,

Gretta N. Rowold
Chair
Email: auecogroup@gmail.com
Website: http://aueco.org