April 14, 2016

Office of Management and Budget
Desk Officer for DoD
Room 10236
New Executive Office Building
Washington, DC 20503

By Federal eRulemaking Portal: http://www.regulations.gov

RE: Docket ID: DARS-2015-0039; Agency: Defense Acquisition Regulations System (DARS) [RIN 0750-AI61 Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS 252.204-7012 DEC 2015)]

Dear Ms. Seehra,

I am writing on behalf of the Association of University Export Control Officers (AUECO), an association of over 155 senior export practitioners with export compliance responsibilities at more than 100 accredited institutions of higher education in the United States. As expressed in its founding charter, AUECO is committed to monitoring changes in the administration of export laws and other regulations that could affect transactions and collaborations in academia.

OMB has requested comments on a proposed data collection burden resulting from:

a. The clause at DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors to report cyber incidents that affect a covered contractor information system or the covered defense information residing therein.

(ii) (D) "cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

AUECO is providing the following comments in response to the Safeguarding Covered Defense Information, Cyber Incident Reporting, and Cloud Computing; Defense Federal Acquisition Regulation Supplement (DFARS) Parts 204 and 239, and related clauses at DFARS 252; OMB Control Number 0704-0478..

It is our opinion that the DFAR clause 252.204-7012 definition of "Cyber incident" is vague and overly broad. As a result, the level of effort required for reporting has not been accurately predicted, and the information that is reported may have no practical utility. Our reading of the existing definition of "Cyber incident" encompasses a wide spectrum from scans of our network by third parties to an actual system breach. Institutions of Higher Education receive thousands of third party system scans a year. Although we are aware of the scans, we do not know what, if any, information is collected from those scans. Requiring reporting on every system scan not only results in data with no practical utility, but also creates a heavy reporting burden for each institution.

In addition, as it is currently written, a legitimate and authorized system patch that "fails" and results in an "adverse effect" would be considered a "Cyber incident." However, we believe reporting on an internal system error is not the intended purpose of the DFARS 7012 clause. In fact, reporting on "Cyber incidents" like the one described above and anticipating other legitimate internal actions which may trigger reporting requirements will consume valuable

institutional resources that would be better spent on identifying outside threats to the institution's information system.

We propose a tiered approach to defining "Cyber incidents"

Cyber Event: An action taken through the use of computer networks that may result in potentially adverse effects or anomalous behaviors on an information system and/or the information residing therein.

Cyber Incident: An action taken through the use of computer networks that results in a compromise of the confidentiality, integrity, and/or an unscheduled or unplanned compromise of availability of an information system and/or the information residing in the system.

Suggested required actions:

1. Collect and monitor "Cyber Event" information
2. Collect, monitor, and report to agency "Cyber Incident" information

If modifying the definition of "Cyber incident" in the manner suggested here is not desired, we request that the agency expand and clarify what constitutes a "compromise" and an "adverse event" in the current definition to allow for a more consistent and accurate prediction of the reporting effort required.

OMB has also requested comments on a proposed data collection burden resulting from:
b. The provision at DFARS 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, requires an offeror that proposes to deviate from any of the security controls of National Institute of Standards and Technology Special Publication 800-171 in effect at the time the solicitation is issued, the offeror must submit to the contracting officer a written explanation of how the specified security control is not applicable or an alternative control or protective measure is used to achieve equivalent protection

Requirements of DFARS 252.204-7008 and 252.204-7012
Institutions of higher education realize a substantial burden complying with the 252.204-7008 at solicitation phase to identify and propose alternate but equally effective security measures on covered contractor information systems. The following is a list of problems faced addressing this requirement at solicitation phase:

- This clause requires significant human resources of IT professionals on the order of twenty (20) to eight five (85) man hours of effort analyzing information system configurations and adapting for compliance with the NIST SP 800-171.

- Concentrating such human resources at solicitation phase does not provide a useful return on investment due to the fact that not all solicitations are awarded. In fact, success rates of solicitations-to-awards tend to be about 25%, meaning that 3 in 4 instances of expending 20-85 man hours to comply with 252.204-7008 is completely wasted.

- Organization-wide plans for alternative but equally effective security measures are subject to approval of each Contracting Officer which leaves risks that plans to uniformly comply with the 252.204-7008 can be rejected on a contract-by-contract basis. In instances where CO's reject certain measures, inefficiencies will arise that will require additional costs in either technology-based solutions, human-resource efforts, or both on a case by case basis.

In addition to the above-cited complexities complying with 252.204-7008 at solicitation phase, the contract clause at 252.204-7012 seems to offer a conflicting set of requirements by allowing "an authorized representative of the

DoD CIO" to determine if alternate but equally effective security measures are acceptable at the award phase as opposed to the Contracting Officer making determinations at the solicitation phase. Also, the 252.204-7012 contract clause takes effect at award phase where the above-identified human resource effort is more justifiable to analyze systems and comply with NIST SP 800-171. Finally, the 252.204-7012 contract clause authorizes a phase-in period up to December 31, 2017 to fully comply with NIST SP 800-171, allowing organizations time to evaluate the requirements and implement a plan to either fully comply by the specified date or propose alternate but equally effective security measures as organizational policy or procedure for how to comply.

The requirements to identify alternate but equally effective security measures to individual controls defined in NIST SP 800-171 is not a practical exercise at solicitation phase, particularly when the opportunity to do so at award phase through a different approval process exists. A more practical solution would be to harmonize the requirements between the DFARS 252.204-7008 and 252.204-7012 to defer efforts to award phase, as they are currently written in the 252.204-7012 contract clause. An alternative solution would be to eliminate the 252.204-7008 clause in solicitations entirely or modify the clause to merely acknowledge the 252.204-7012 will apply to the resultant contract (e.g., remove subpart (c) from 252.204-7008).

The data request would be more useful if it were modified to collect data on a clause with harmonized definitions and requirements. The affected public should also be asked about the change in burden if the DFAR 252.204-7008 reporting requirement were removed.

AUECO appreciates the opportunity to provide the Office of Management and Budget of State with the above comments on Docket ID: DARS-2015-0039; Agency: Defense Acquisition Regulations System (DARS) [RIN 0750-AI61 Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS 252.204-7012 DEC 2015)].

Sincerely,

Brandi Boniface

Chair
Association of University Export Control Officers
Website: http://aueco.org