VIA REGULATORY PORTAL AND ELECTRONIC MAIL

Leigh Pomponio
NASA Headquarters
Office of Procurement
Contract Management Division
Washington, D.C. 20546


Dear Ms. Pomponio:

On behalf of the Section of Public Contract Law of the American Bar Association (the Section), I am submitting comments on the above-referenced Proposed Rule: Release, Handling, and Protection of Restricted Information (hereafter “Proposed Rule”). The Section consists of attorneys and associated professionals in private practice, industry, and Government service. The Section’s governing Council and substantive committees have members representing these three segments, to ensure that all points of view are considered. By presenting their consensus view, the Section seeks to improve the process of public contracting for needed supplies, services, and public works.

The Section is authorized to submit comments on acquisition regulations under special authority granted by the Association’s Board of Governors. The views expressed herein have not been approved by the House of Delegates or the

1 The Honorable Thomas C. Wheeler, a member of the Section’s Council, did not participate in the Section’s consideration of these comments and abstained from the voting to approve and send this letter.
Board of Governors of the American Bar Association and, therefore, should not be construed as representing the policy of the American Bar Association.2

The Section recognizes that the National Aeronautics and Space Administration (NASA) has various directives and regulations that address the protection or release of unclassified information. The Section appreciates that NASA has made an effort through the Proposed Rule to clarify and better reflect NASA’s existing policy. The Section nevertheless encourages NASA to broaden its efforts to include other federal agencies that have regulations or guidance addressing protection and release of various categories of unclassified information. The Section attaches to this letter its comments on the Department of Defense (DoD) Advance Notice of Proposed Rulemaking: Safeguarding Unclassified Information (DFARS Case 2008–D028; 75 Fed. Reg. 9563 (Mar. 3, 2010)) to convey the substance of our comments because both the DoD and NASA rulemakings present similar issues. Both DoD and NASA identify new definitions and categories of Controlled Unclassified Information, which the Section is concerned will create confusion. The Section offers these comments to assist NASA in better implementing a government-wide policy.

The Section is available to provide additional information or assistance as you may require.

Respectfully submitted,

Karen L. Manos,
Chair, Section of Public Contract Law

Attachment

cc: Donald G. Featherstun
Carol N. Park Conroy
Mark D. Colley
David G. Ehrhart
Allan J. Joseph
John S. Pachter
Michael M. Mutek
Patricia A. Meagher

2 This letter is available in pdf format at: http://www.abanet.org/contract/regscomm/home.html under the topic “Emerging Areas.”
Council Members, Section of Public Contract Law
Chairs of the Cybersecurity, Privacy and Data Protection Committee
Kara M. Sacilotto
VIA REGULATORY PORTAL AND ELECTRONIC MAIL

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


Dear Mr. Thrash:

On behalf of the Section of Public Contract Law of the American Bar Association (the Section), I am submitting comments on the above Advanced Notice of Proposed Rulemaking: Safeguarding Unclassified Information (hereafter “ANPR”).1 The Section consists of attorneys and associated professionals in private practice, industry, and Government service. The Section’s governing Council and substantive committees have members representing these three segments, to ensure that all points of view are considered. By presenting their consensus view, the Section seeks to improve the process of public contracting for needed supplies, services, and public works.

The Section is authorized to submit comments on acquisition regulations under special authority granted by the Association’s Board of Governors. The views expressed herein have not been approved by the House of Delegates or the

---

1 The Honorable Thomas C. Wheeler, a member of the Section’s Council, did not participate in the Section’s consideration of these comments and abstained from the voting to approve and send this letter.
Board of Governors of the American Bar Association and, therefore, should not be construed as representing the policy of the American Bar Association.  

The Section recognizes that the Department of Defense (DoD) has various directives and regulations that address the protection or release of unclassified information. The Section appreciates that DoD has made an effort to consolidate this guidance under two Department of Defense Federal Acquisition Regulation Supplement (DFARS) clauses. The Section nevertheless encourages DoD to broaden its efforts to include other federal agencies that have regulations or guidance addressing protection and release of unclassified information. The Section offers these comments to assist DoD in better implementing a government-wide policy.

I. BACKGROUND

The ANPR points out that the DFARS presently does not address the safeguarding of unclassified DoD information within industry, nor does it address cyber intrusion reporting for that information. The stated purpose of the DFARS changes is “to implement adequate security measures to safeguard DoD information on unclassified industry information systems from unauthorized access and disclosure, and to prescribe reporting to the Government with regard to certain cyber intrusion events that affect DoD information resident or transiting on contractor unclassified information systems.” 75 Fed. Reg. at 9564. The ANPR includes two proposed DFARS clauses and also announces a public meeting to be held on the subject on April 22, 2010.

Another policy addressing the safeguarding of unclassified information has its roots in a December 16, 2005, Presidential Memorandum, “Guidelines and Requirements in Support of the Information Sharing Environment,” 3 issued with a stated goal of creating an Information Sharing Environment (ISE) to facilitate the sharing of terrorism information.

In response to the Presidential Memorandum, officials soon discovered that “there are at least 107 unique markings” for unclassified information “and more than 131 different labeling or handling processes,” according to testimony in April

---

2 This letter is available in pdf format at: http://www.abanet.org/contract/regscomm/home.html under the topic “Emerging Areas.”

2007 by Ambassador Thomas E. McNamara, then Program Manager of the Office of the Director of National Intelligence (ODNI) ISE.  

In some cases the very same markings are used to refer to different control systems, Mr. McNamara explained. Thus, SSI usually means “Sensitive Security Information,” but sometimes it stands for “Source Selection Information.” Likewise, some agencies use ECI to designate “Export Controlled Information,” while others use it to mean “Enforcement Confidential Information,” each of which entail “very different safeguarding and dissemination controls.” In short, the handling of unclassified information within Government had become chaotic and counterproductive. This is particularly the case for the Government’s contractors that may have contracts with multiple agencies.

On May 9, 2008, President Bush issued a memorandum entitled “Designation and Sharing of Controlled Unclassified Information.” The memorandum stated its intent:

This memorandum (a) adopts, defines, and institutes “Controlled Unclassified Information” (CUI) as the single, categorical designation henceforth throughout the executive branch for all information within the scope of that definition, which includes most information heretofore referred to as “Sensitive But Unclassified” (SBU) in the Information Sharing Environment (ISE), and (b) establishes a corresponding new CUI Framework for designating, marking, safeguarding, and disseminating information designated as CUI. The memorandum’s purpose is to standardize practices and thereby improve the sharing of information, not to classify or declassify new or additional information.

*Id. at ¶ 1.*

The memorandum goes on to describe the markings that may be used to identify CUI:

(7) All CUI shall be

---


5 *Id. at 2.*

(a) categorized into one of three combinations of safeguarding procedures and dissemination controls, and

(b) so indicated through the use of the following corresponding markings:

(i) “**Controlled with Standard Dissemination**” meaning the information requires standard safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it is reasonably believed that it would further the execution of a lawful or official purpose.

(ii) “**Controlled with Specified Dissemination**” meaning the information requires safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Material contains additional instructions on what dissemination is permitted.

(iii) “**Controlled Enhanced with Specified Dissemination**” meaning the information requires safeguarding measures more stringent than those normally required since the inadvertent or unauthorized disclosure would create risk of substantial harm. Material contains additional instructions on what dissemination is permitted.

(8) Any additional CUI markings may be prescribed only by the Executive Agent. Use of additional CUI markings is prohibited unless the Executive Agent determines that extraordinary circumstances warrant the use of additional markings.

*Id.* at ¶¶ 7 & 8.

The memorandum defines the “Executive Agent” that must approve any additional CUI markings as the National Archives and Records Administration (NARA). *Id.* at ¶ 3(g).

A briefing given April 6, 2009, by Ms. Deborah Ross, Deputy Director, Information Security Policy Office of the Under Secretary of Defense (Intelligence) and Ms. Roberta Schoen, Director of Operations Defense Technical Information Center set forth DoD’s plans to implement the new CUI approach by 2013.7

---

7 Available at [www.dtic.mil](http://www.dtic.mil)
II. COMMENTS

A. The Creation of a New Category of Information Adds to the Confusion Contractors Face When Marking and Safeguarding CUL.

The ANPR proposes a new defined term, “DoD Information” to mean:

“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.

75 Fed. Reg. at 9566.

While this new term is codifying in the DoD procurement regulations what already exists in a DoD Directive, it adds to the confusion over what to call, how to mark, and how to treat unclassified information that may not be released to the public.\(^8\) The Section strongly encourages DoD to wait until government-wide guidance is available to issue more regulations on this subject.


DoD faces a difficult challenge in mandating improvements to industries’ cybersecurity posture. As an organization of attorneys, we do not attempt to comment on the substance of the cybersecurity measures proposed. From the perspective of government contracts attorneys and associated professionals in

\(^8\) The day after the ANPR was released the National Aeronautics and Space Administration (NASA) issued a proposed rule changing the name of unclassified information not to be released to the public from “sensitive information” to “restricted information.” 75 Fed. Reg. 9860 (Mar. 4, 2010).
government, industry and private practice, however, the Section foresees policy and implementation issues that would affect all parties.

First, it is very unlikely that the regulatory process will be able to keep up with the constantly evolving threat. A reasonable precaution today may not be sufficient next month. Rather than include cybersecurity requirements in a DFARS clause that may quickly become out of date and require extensive time and resources to amend, the Section recommends including these requirements in a stand-alone standard or specification that could be incorporated by reference. Adoption of one of the existing commercial standards would require the least effort for DoD, if it satisfies DoD’s needs.

Second, a reasonable level of cybersecurity necessarily involves a trade-off between the potential losses from cyber events, and the real costs of implementing additional security measures in terms of capital investments, operation and maintenance, and losses in productivity. We suggest that DoD provide some discussion of this analysis because DoD will directly or indirectly bear a significant share of the costs of cyber defense.

Third, contractors need some certainty about their contractual obligations at the time of award. The necessary actions described in the ANPR are not sufficiently specific to serve as contract clause requirements. They include undefined commitments and are open-ended and ambiguous. Clauses that are open to multiple interpretations often lead to disagreements and disputes. For example, the statement that undesignated information must be protected as though it is designated is confusing. See 204.7XX2(d)(ii),(iv) & (v). We recommend that DoD personnel be required to mark information that must be protected to avoid needless controversy.

Fourth, systems breaches are inevitable, even in IT systems maintaining high standards of security. Therefore, we are concerned that the draft language implies that by reporting a cyber intrusion, a contractor is increasing its risk of being found noncompliant with contract requirements. Should DoD truly wish to receive reports of all cyber intrusions involving CUI, the Section suggests that contractors that make cyber intrusion reports be offered a safe harbor. Those contractors with unusually frequent or severe cybersecurity breaches may need the adequacy of their security systems reviewed, but “[a] cyber intrusion event” alone should not trigger scrutiny.

One approach to addressing the tension between a rapidly evolving threat, rapidly evolving defensive measures, and a contractor’s need for certainty would be to empower a government/industry working group to develop and keep current best
practices or an industry standard that represent a “safe harbor.” Such practices would be equally applicable to both government and industry IT systems, and if implemented, would satisfy the contractual obligation for reasonable security measures required by the contract clause. DoD would not need to include the details of reasonable security measures in the clause; indeed, given the evolving nature of the threat, it is a challenge to do so. Instead, it would require a system that implements reasonable measures, and provide a source of such measures that a contractor could implement to meet its contractual obligation. This approach is similar to that taken for other contractor required systems, such as Earned Value, Material Management Accounting Systems, Quality Assurance, and others.

III. CONCLUSION

The Section applauds the fact that DoD has used the notice and comment process and hosted a public meeting to understand the potential impact of the proposed rule. These comments are meant to propose improvements on the DoD’s implementation effort and encourage DoD to continue to seek out the assistance of other agencies and the public in the process of refining these contract clauses. The Section respectfully requests that DoD consider the issues identified in these comments in developing a proposed DFARS rule to address safeguarding of certain unclassified information. The Section appreciates that the ANPR codifies DoD’s existing Directives regarding the safeguarding of unclassified information that may not be released to the public, but suggests that any new rule should conform to the new Controlled Unclassified Information designation, provide unambiguous guidance, and include specifics in a separate standard or specification.
The Section is available to provide additional information or assistance as you may require.

Respectfully submitted,

Karen L. Manos,
Chair, Section of Public Contract Law

cc: Donald G. Featherstun
Carol N. Park Conroy
Mark D. Colley
David G. Ehrhart
Allan J. Joseph
John S. Pachter
Michael M. Mutek
Patricia A. Meagher
Council Members, Section of Public Contract Law
Chairs of the Cybersecurity, Privacy and Data Protection Committee
Kara M. Sacilotto