Via Email to sec809@dau.mil

November 20, 2017

Section 809 Panel
Ms. Diedre Lee, Chair
Mr. David Drabkin, Commissioner, Team 4
1400 Key Blvd.
Suite 210
Rosslyn, VA 22209

Re: Comments to Section 809 Panel; Cybersecurity Provisions

Dear Ms. Lee and Mr. Drabkin:

On behalf of the American Bar Association (“ABA”) Section of Public Contract Law (“Section”), I am submitting comments to assist the Section 809 Panel in reviewing acquisition regulations applicable to the Department of Defense (“DoD”) with a view towards streamlining and improving the efficiency and effectiveness of defense acquisition and defense technology advantage, along with achieving related goals. The Section consists of attorneys and associated professionals in private practice, industry, and government service. The Section’s governing Council and substantive committees include 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 views expressed herein are presented on behalf of the Section. They have not been approved by the House of Delegates or the Board of Governors of the ABA and, therefore, should not be construed as representing the position of the ABA.2

1 Mary Ellen Coster Williams, Section Delegate to the ABA House of Delegates, and Marian Blank Horn, Kristine Kassekert, and Heather K. Weiner, members 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.

2 This letter is available in pdf format at http://www.americanbar.org/groups/public_contract_law/resources/prior_section_comments.html under the topic “Cybersecurity; Access to and Protection of Information.”
I. INTRODUCTION

This comment letter for the Section 809 Panel focuses on the impact of DoD’s Network Penetration Reporting and Contracting for Cloud Services (Case 2013-D018), and the corresponding clause, DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (“CDI Rule”).

The Section has submitted robust comments to DoD on the CDI Rule, dating back to the initial iteration proposed in 2011. Many themes raised in the Section’s prior comments still apply to the panel’s current inquiry. Below are four key considerations that the Section believes are critical to accomplishing the panel’s objectives of increasing efficiency and minimizing the burdens imposed by the current regulatory landscape with regard to cybersecurity regulations.

II. COMMENTS

The comments below are offered based on lessons learned in implementing the CDI rule.

A. The Section recommends that the Section 809 Panel ensure that new cybersecurity and information security rules build in sufficient time for contractors to adjust to new and revised standards and incorporate them into internal systems and procedures.

The Section offers as an example the application of National Institute of Standards and Technology (“NIST”) Special Publication (“SP”) 800-171 through an interim version of the DFARS CDI Rule in August 2015.3 The chain of events related to that rule demonstrates the need for sufficient lead time when implementing changed standards. The interim rule applied the SP 800-171 standards effective immediately. DoD later extended the implementation deadline to December 31, 2017 in response to the concerns raised by industry. As the Section explained in its October 2015 comments on the interim CDI Rule, DoD had essentially asked contractors to comply with an entirely new information-security framework, with complex and demanding requirements, immediately—while in contrast federal agencies received an entire year to comply with updates to existing requirements under the Federal Information Security Management Act. This type of rulemaking imposes serious burdens on contractors and barriers to entry for potential contractors, including those that may have supplies or services that would provide DoD technological advantages. The government-contracting community has finite resources to allocate to compliance with changing standards. Thus, DoD must build in sufficient tools and lead time for contractor compliance.

3 The Section notes that it was not until September 2016 that the National Archives and Records Administration (“NARA”) issued its final version of a Controlled Unclassified Information (“CUI”) rule “to standardize the way the executive branch handles information that requires safeguarding or dissemination controls (excluding information that is classified)” under authority listed in the publication; that standard was made effective November 14, 2016. See 81 Fed. Reg. 63324 (September 14, 2016).
B. **The Section recommends that the Section 809 Panel consider the disproportionate impact on small to medium-sized contractors of such requirements.**

The Section raised its concerns during prior DoD comment periods regarding the barriers to entry created by burdensome cybersecurity requirements and the disproportionate impact that such requirements have on small and mid-sized contractors. The Section’s concern is that these requirements may cause such companies to avoid the market entirely. There is a similar detrimental impact throughout the supply chain, with regard to commercial contractors and subcontractors for whom federal work represents only a small share of their business. For both groups, these rules and the short period of time to become compliant represent an increased barrier to entry and burdens to compliance that have the possibility of eliminating such groups in their entirety.

Additionally, even if such companies do elect to remain in the government contracting market, small to medium-sized businesses may lack the access of larger organizations to customer agencies or more sophisticated prime contractors. This comparative lack of access can increase the likelihood of such groups’ noncompliance if, for example, a small business prime cannot work effectively with a customer agency to more clearly define the CUI that needs to be safeguarded (at the prime level and at the subcontracting level), or to propose and negotiate a variance if necessary.

C. **The Section recommends that the Section 809 Panel work closely with industry to ensure that any such cybersecurity and information reporting requirements are feasible.**

The Section’s previous comments on the interim CDI rule requested that DoD consider reviewing whether the rule’s across-the-board 72-hour reporting requirement was feasible and asked that DoD better balance its desire for timely information against the quality of the information that a contractor could reasonably provide within that timeframe. The Section believes that this point remains valid for the panel’s consideration, particularly because many states provide substantially longer timeframes or more situation-dependent timeframes such as “without undue delay,” instead of a flat 72-hour window.

Moreover, as with the other requirements of the CDI Rule, the reporting requirements raise several questions about prime-sub relationships, such as the amount of detail to be shared by the parties following an incident and whether there are any safe harbor provisions between sub and prime contractors in exchange for the subcontractor’s willingness to provide more detail to the prime about the incident in question during these early stages. The reporting flow-down obligations mandate notification to the prime contractor in the event of a report made by a subcontractor directly to the Government, but the primes lack the same degree of access and information to be able to assess the risk to the prime contractor and the Government from their vantage point.

These are not merely issues to be resolved among prime contractors and subcontractors. Without coordination of the 72-hour timeframe and the lack of clarity on what constitutes CDI
under a particular contract or subcontract (another point the Section has raised in comments to DoD), there is a risk that prime contractors and subcontractors will report cyber incidents inconsistently (i.e., with a prime contractor having one understanding of an incident affecting CDI and the subcontractor having another). Without coordination and clarity from DoD on the issues set forth in these and other comments submitted from the Section to date, more questions than answers may be triggered by the 72-hour reporting requirement.

**D. There is a continued need for ongoing education within the Government on the intended operation of the rule to ensure smooth implementation.**

Finally, the Section notes that the recent dialogue between DoD and industry has revealed a disconnect between (a) the expectations the parties drafting the regulations may have had about program offices’ roles in the process, and (b) the program offices’ understanding of their responsibilities. Contractors at all levels continue to grapple with assessing whether the safeguarding obligations have been triggered (e.g., whether information is, in fact, CUI). And, critically, the fact that the CDI Rule was issued before DoD published internal guidance defining CUI—guidance which remains unpublished to this day—underscores the need for internal training and dialogue.

DoD has confirmed that it is the agency’s responsibility to make that determination, but the Section believes that there is a strong need for training within the Government to identify accurately and clearly what constitutes CUI. Absent DoD training and agencies’ expressly identifying CUI for particular procurements, contractors are left to assess this information on their own. Simply pointing contractors to the CUI Registry on the NARA website, which includes many CUI categories, has not proven workable in practice because it leaves contractors unable to make a risk determination about which information the contracting entity wants protected under the rule.

This arrangement could lead to diverging interpretations of the information covered as CDI, which systems must be compliant under the CDI Rule, and how those systems must comply. And this arrangement could result in contractors’ seeking clarification after the fact through contracting officers, who may not be the most qualified or knowledgeable personnel to render these judgments and who already have limited time to perform contract procurement and administration duties. Thus, it is important that DoD direct program offices, which the DoD has confirmed will have primary responsibility for either identifying or confirming that information

---

4 DoD held an Industry Information Day to brief and receive input on its implementation of the CDI Rule. See 82 Fed. Reg. 16577 (April 5, 2017). The Section applauds DoD’s hosting such information-sharing opportunities. It is the Section’s sincere hope that industry days are not used only after the fact to discuss the meaning and implementation of significant rules, such as the CDI rule, but that they are also used on the front end to develop better regulations and ameliorate implementation concerns such as those identified in this letter.

5 The CDI Rule was issued before NARA crafted its own rule as well. See note 3, *supra*.


7 DFARS 252.204-7012(a) (refers contractors to http://www.archives.gov/cui/registry/category-list.html).
is in fact CDI, to make their CDI determinations early and to coordinate with the contractor and the Contracting Officer to ensure that there is a clear record of the information and systems subject to these requirements.

The Section requests that the panel recommend that DoD work internally between program and contracting offices to recognize that for this process to work effectively, the requiring activities and contracting activities must agree on the information requiring protections. To that end, it would help for DoD to have developed underlying and related guidance such as how to identify and mark controlled unclassified information before requiring contractors to comply with and flow down requirements contingent on these definitions. As noted above, leaving prime contractors to grapple with these definitional issues is not an optimal way to implement the rule and is bound to introduce inconsistency and the risk of noncompliance. Failing to provide this guidance also increases the tensions between prime and subcontractors. Both primes and subcontractors no doubt will have an interest in the Government’s being coordinated and consistent—particularly before contract award—on what constitutes CDI, and which party under a contract/subcontract will handle CDI with the concomitant obligation to safeguard and report any incidents affecting the CDI.

III. CONCLUSION

The Section appreciates the opportunity to provide feedback to the Section 809 Panel to inform the Panel’s efforts to streamline the contracting process. The Section is available to provide additional information or assistance as you may require.

Sincerely,

Aaron Silberman
Chair, Section of Public Contract Law

cc:
Kara M. Sacilotto
Linda Maramba
Susan Warshaw Ebner
Annejanette Heckman Pickens
Council Members, Section of Public Contract Law
Chairs and Vice Chairs, Acquisition Reform and Emerging Issues Committee
Chairs and Vice Chairs, Cybersecurity Committee
Craig Smith
Samantha S. Lee