December 16, 2011

VIA REGULATORY PORTAL AND ELECTRONIC MAIL

Defense Acquisition Regulations System
Attn: Mr. Julian Thrash
OUSD (AT&L), DPAP (DARS)
Room 3B855
3060 Defense Pentagon
Washington, DC 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 Proposed Rulemaking: DFARS Case 2011-D039; Safeguarding Unclassified DOD Information, 76 Fed. Reg. 38089 (June 29, 2011) (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.¹

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.
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 the efforts DoD has made with respect to this guidance and commends DoD for the improvements to the Proposed Rule over the Advance Notice of Proposed Rulemaking (“ANPR”) that make the Proposed Rule clearer. It also is apparent to the Section that DoD had taken into account many of the comments it received. The Section nevertheless encourages DoD to broaden its efforts to consider the experiences of other federal agencies that have regulations or guidance addressing information protection and release of unclassified information and offers these comments to assist DoD in better implementing a government-wide policy.

I. COMMENTS

The stated purpose of the Proposed Rule “is to implement adequate security measures to safeguard unclassified DoD information within contractor information systems from unauthorized access and disclosure, and to prescribe reporting to DoD with regard to certain cyber intrusion events that affect DoD information resident on or transiting through contractor unclassified information systems.” 76 Fed. Reg. 38090. As noted in our comments to the ANPR, defining through regulation improvements to industry’s cybersecurity practices presents a challenge because of: (i) the constantly evolving nature of the cybersecurity threat; (ii) the necessary trade-off between the potential losses from cyber events and the significant costs in terms of adding security measures; (iii) contractors’ need to understand their contractual obligations at the time of award; and (iv) the reality that cybersecurity incidents are inevitable, even if a contractor maintains a high standard of security.

The Section’s comments address five areas intended to improve the final rule: (1) the scope of the Proposed Rule; (2) clarifications to definitions; (3) the roles and responsibilities of the parties; (4) the legal protections provided to parties that suffer cyber incidents; and (5) the technical requirements that the rule may impose on contractors. As an initial matter, as noted in the background section to the Proposed Rule, the National Archives and Records Administration is currently leading an effort regarding the classification and marking of controlled unclassified information. The background section of the Proposed Rule acknowledges that the results of this effort may require modification of any DFARS rule in this area. 76 Fed. Reg. 38090. To avoid confusion and in light of the expenditures contractors will likely need to make to comply with a DFARS clause, we encourage DoD to

---

2 This letter is available in pdf format under the topic “Cybersecurity; Access to and Protection of Information” at: www.americanbar.org/groups/public_contract_law/resources/prior_section_comments.html.
wait until this government-wide guidance is available before issuing an interim or final regulation on this subject. This is especially appropriate given the mandate in the Federal Information Security Management Act of 2002 ("FISMA") that the cost-effectiveness of security protocols should be considered. See 44 U.S.C. § 3544(a)(2)(C) ("implementing policies and procedures to cost-effectively reduce risks to an acceptable level"); see also id. § 3544(b)(2)(B).

A. The Section Recommends Narrowing The Proposed Rule

1. The Section Recommends that DoD Revise and Clarify the Description of Technical Data Covered by the Proposed Rule

Although the Section recognizes the efficiency of having one rule govern all types of unclassified information that should be protected in some way, the Section is concerned with the propriety of requiring the same level of protection for third-party proprietary information as that proposed for information that bears on national security, such as munitions list export control information. For example, the Proposed Rule requires Enhanced Safeguarding procedures for "Technical data, computer software, and any other technical information covered by DoD Directive 5230.24, Distribution Statements on Technical Documents, and DoD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure." DFARS 204.7402(d)(2)(vi) (proposed). Given the scope of this DoD Directive, it is not clear that this DoD Directive is applicable to all information at issue in the Proposed Rule. DoD Directive 5230.24 states that it:

covers newly created technical documents generated by all DoD-funded research, development, test and evaluation (RDT&E) programs, which are the basis of the DoD Scientific and Technical Information Program (STIP) described in reference (b). This Directive also applies to newly created engineering drawings, standards, specifications, technical manuals, blueprints, drawings, plans, instructions, computer software and documentation, and other technical information that can be used or be adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment.

DoD Directive 5230.24, ¶ 2.2 (emphasis added).

The technical data and computer software included within the second sentence quoted above is significant. This portion of the Directive also arguably conflicts with the definition of DoD Information in the Proposed Rule, which states that DoD Information is limited to the nonpublic information that is received from DoD or is directly related to "support of an official DoD activity." DFARS 252.204-7000 (a). The reference to technical data and computer software that
could be adapted for use as military or space equipment or technology appears to go beyond information related to an official DoD activity and may encompass information that a commercial company most likely would have difficulty identifying.

The Proposed Rule may also conflict with DoD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure, which the Proposed Rule relies upon to define the information covered. DFARS 204.7402(d)(2)(vi) (proposed). Specifically, DoD Directive 5230.25 states that it:

2.2.2. Does not modify or supplant the regulations promulgated under E.O. 12470 (reference (b)) or the Arms Export Control Act (reference (c)) governing the export of technical data, that is, 15 CFR 379 of the Export Administration Regulations (EAR) (reference (f)) and 22 CFR 125 of the International Traffic in Arms Regulations (ITAR) (reference (g)).

2.2.3. Does not introduce any additional controls on the dissemination of technical data by private enterprises or individuals beyond those specified by export control laws and regulations or in contracts or other mutual agreements, including certifications made pursuant to subsection 3.2., below. Accordingly, the mere fact that the Department of Defense may possess such data does not in itself provide a basis for control of such data pursuant to this Directive.

2.2.4. Does not introduce any controls on the dissemination of scientific, educational, or other data that qualify for General License GTDA under subsection 379.3 of the EAR (reference (f)) (see enclosure E3.) or for general exemptions under subsection 125.11 of the ITAR (reference (g)) (see enclosure E4.).

2.2.5. Does not alter the responsibilities of DoD Components to protect proprietary data of a private party in which the Department of Defense has “limited rights” or “restricted rights” (as defined in subsections 9-201(c) and 9-601(j) of the DoD Federal Acquisition Regulation Supplement, reference or which are authorized to be withheld from public disclosure under 5 U.S.C. 552(b) (4) (reference (i)).

2.2.6. Does not pertain to, or affect, the release of technical data by DoD Components to foreign governments, international organizations, or their respective representatives or contractors, pursuant to official agreements or formal arrangements with the U.S. Government, or pursuant to U.S. Government-licensed transactions involving such entities or individuals. In the absence of such U.S.
Government-sanctioned relationships, however, this Directive does apply.

DoD Directive 5230.25 ¶ 2.2.2-2.2.6.

The Proposed Rule, by contrast, adds controls and responsibilities with respect to what is defined as DoD Information that may be inconsistent with these paragraphs of DoD Directive 5230.25. To avoid potential confusion or conflict with these DoD Directives, the Section suggests that these DoD Directives be used as references and not incorporated into the final rule. Because all subsets of data addressed by the two DoD Directives are covered with specificity elsewhere in the Proposed Rule, it also is not necessary for the Directives to be incorporated in their entirety.

2. The Section Recommends that DoD Revise the Rules with respect to Third Party Information

Many organizations have standard commercial practices already in place to define how third party proprietary information should be protected. In addition, companies routinely enter into non-disclosure agreements, teaming agreements, licensing agreements, and subcontracts that identify proprietary information that will be exchanged and how it should be protected and handled. This model is well developed and understood.

The Proposed Rule could disrupt this established practice by applying the enhanced safeguarding standards to contractors and their team members that possess third party proprietary information, but no other type of DoD Information. As discussed further below (Part E), these enhanced safeguarding standards include many features that contractors will already use, but, as written, they also appear to require that each company subject to the enhanced safeguarding clause will need to implement a “Common Access Card” (“CAC”), like a public key infrastructure (“PKI”) system, on their unclassified networks. This feature could be time-consuming and expensive to integrate for some contractors. Because most contractors doing business with DoD exchange proprietary information with third parties at some point, inclusion of third party proprietary information could impose the enhanced safeguarding standard more broadly than necessary to protect DoD Information.

In addition, application of the enhanced safeguarding requirements to all third party proprietary information exchanges may dissuade commercial item exchanges.

---

3 Our comments in this section relate to third party proprietary information that contractors obtain from each other during the course of their commercial and business transactions, such as through teaming agreements or subcontract work. We are not addressing third party information that contractors receive from the Government in the course of performing a government contract.
Defense Acquisition Regulations System  
Attn: Mr. Julian Thrash  
OUSD (AT&L), DPAP (DARS)  
Page 6 of 13

contractors from entering into business with DoD. In an effort to limit the Government’s regulatory requirements on their overall business, some commercial item vendors perform only commercial item subcontracts in connection with government contracts. These commercial item subcontractors likely have entered into a commercial agreement with their prime contractor to prescribe how proprietary information should be treated and protected. Application of the enhanced safeguarding standard to these subcontractors may impose additional compliance burdens that could lead some commercial item contractors to withdraw from the federal marketplace.

Small businesses may also be discouraged from contracting with DoD. Some small businesses may have only one or two contracts that involve DoD Information and, as a result, third party proprietary information may be the only type of DoD Information in their possession. The costs of implementing the enhanced safeguarding standard may be disproportionately costly for these small businesses and dissuade them from pursuing DoD contracts.

Accordingly, the Section recommends that DoD exclude third-party proprietary information that contractors exchange with each other from the definition of “DoD information.” The Section believes that the commercial agreements between private parties currently, and will continue to, provide a sufficient standard of protection for this information.

3. The Section Recommends that DoD Modify the Requirement to Use the “Best Level” of Security Available

The proposed clause at 252.204-70XX on the basic safeguarding of unclassified DoD information “requires the transmittal of electronic communications “using technology and process that provides the best level of security and privacy available, given facilities, conditions, and environment.” (Emphasis added). The stated purpose of the Proposed Rule, however, is to provide for adequate security, a concept that is also embedded in proposed Subpart 204. See, e.g., Proposed DFARS 204.702(a). The proposed “best level available” standard also is not a defined term of art, and a comparable standard does not exist under the National Institute of Standards and Technology (“NIST”) standards, Federal Information Processing Standards (“FIPS”), or FISMA. Because of the evolving nature of cybersecurity threats, new technology and processes are currently being developed and will continue to be developed. Because of the significant cost and lead time necessary to implement new technology and processes, a standard based on the “best level of security and privacy available” will be evolving, difficult to measure, and difficult with which to comply. The Section therefore recommends that DoD replace the phrase “the best level of security and privacy available” with the phrase “adequate security and privacy safeguards.”
B. **The Section Recommends That DoD Clarify The Definitions In The Proposed Rule**

1. **The Term “Incident” Should Be Defined in Subpart 204.74**

   Although Section 204.7401 defines the term “cyber” by reference to the clause at 252.204-70YY, it does not define the term “Incident.” Nevertheless, the term “incident” is defined in the clause at 252.204-70YY. The Section therefore recommends that DoD clarify Section 204.7401 by modifying the section to define the term “incident” by reference to the clause at 252.204-70YY.

2. **The Application of the Subpart to Various Forms of Voice Information Should Be Clarified by the Inclusion of Definitions of “Voice” and “Information” in Subpart 204.74 and Clarification of Proposed Clause 252.204-70XX**

   Although subsection 204.7400(b) states that “[t]his subpart does not apply to voice information,” the Proposed Rule would be improved and its applicability clarified by a definition of the terms “voice” and “information.”

   In addition, assuming that the term “voice information” could be understood as the sum of the definitions of the terms “voice” and “information” in the clause at 252.204-70XX, the Section nevertheless recommends that DoD clarify the term “voice information.” The terms “voice” and “information” arguably result in the collective term “voice information,” meaning any oral communicable knowledge regardless of its transmission protocol (the “oral” limitation establishing the parameters of the “voice” subset within the set of all information). Nonetheless, the combination is also susceptible to other interpretations, particularly in the absence of a clear understanding of what is meant by “transmission protocol” in this context. To prevent such ambiguity, the Section recommends that DoD modify the Proposed Rule to define expressly the collective term “voice information” in the clause at 252.204-70XX. Consistent with the statement in proposed Section 204-7400(b) that the subpart does not apply to “voice information,” we further suggest that the definition clarify whether and to what extent the “voice information” to which the subpart does not apply includes both digital audio recordings of oral information and digital transcripts of the same, including text files generated from an audio recording (e.g. voicemail message) via voice-recognition software and transmitted to a user’s computer or personal digital assistant (“PDA”).

---

4 The Section also suggests that the DoD ensure that its definition of “incident” is consistent with the Division of Corporation Finance, Securities and Exchange Commission CF Disclosure Guidance: Topic No. 2 on Cybersecurity (Oct. 13, 2011).
C. The Section Recommends That DoD Clarify The Roles And Responsibilities Of The Parties

1. The Rule Should Identify How and By Which Entity Audits or Reviews Will Be Conducted

The Proposed Rule should identify which entity will be conducting reviews and audits for the sake of inspection and approval under proposed DFARS 252.204-70XX and 252.204-70YY. Although the Defense Contract Audit Agency (“DCAA”) may have some authority for IT audits under its General IT Audit Rights (see generally CAM 5-500), we are concerned that the DCAA may have neither the experience nor the capacity to take on the new inspections that would be required. Alternatively, audits may fall more under the rubric of the inspections the Defense Security Service (“DSS”) performs for classified systems. As with DCAA, DSS also may lack the capacity to perform additional inspections. Regardless of which entity ultimately has responsibility for auditing compliance with the Proposed Rule, we suggest that the rule would be more clear to both Government and contractors if DoD provided more information regarding the roles and authority various auditing agencies will have.

2. The Rule Should Clarify the Responsibility for Inspecting Subcontractor Systems

DFARS 252.204-70XX(b)(7) states that a contractor may only transfer government information “to those subcontractors that both have a need to know and provide at least the same level of security as specified in this clause.” The Proposed Rule is unclear, however, regarding which party will be responsible for auditing or inspecting the subcontractor’s level of security. As currently drafted, the prime contractor may be responsible for approving the subcontractor’s basic cybersecurity system. Yet, many subcontractors perform work for more than one prime contractor, making it possible that a subcontractor will face conflicting interpretations of the requirements. Given the need for consistency and a minimum level of security, it is reasonable to interpret the Proposed Rule as requiring the Government to perform inspection and approval of subcontractors’ cybersecurity systems. As noted above, however, the Proposed Rule is not clear as to which DoD entity will perform contractor-level audits and, thus in turn, subcontractor-level audits. The Proposed Rule is also unclear whether a prime contractor must wait for a government audit or inspection before transferring DoD Information. If the final rule does not provide for government-performed subcontractor-level audits or assessments, we recommend that the rule be clarified to allow the subcontractor to certify to the prime contractor that the subcontractor’s systems meet the basic requirements of the applicable clause.
3. **DFARS 252.204-7000 Should Be Clarified**

The proposed changes to DFARS 252.204-7000 should be clarified regarding the contracting officer’s role with respect to approving release of DoD Information. In the current version of the DFARS clause, the contracting officer may grant approval for release of information. The Proposed Rule’s version of DFARS 252.204-7000 appears to withdraw the contracting officer’s discretion in this regard and only allows release in specific circumstances, e.g., if the information is required as part of a DCAA audit or Inspector General, Department of Justice, or congressional investigation, if the information is already in the public domain, or if the information results from the performance of a fundamental research project under National Security Decision Directive 189. We recommend that DoD revise the proposed rule to grant contracting officers more discretion for two reasons. First, the rule as revised does not allow for other situations in which contractors may be obligated to release certain information, such as compelled discovery in civil litigation, including civil False Claims Act litigation in which the Department of Justice has not intervened. Second, although the rule appears to have been revised to remove the contracting officer’s authority to grant approval, the Proposed Rule’s version still contains paragraph (c), which discusses the requirements for “requests for approval” including what should be contained in the request and the timing of such a request. If DoD intended to allow for release only in the specified contexts and not by approval of the contracting officer, this paragraph appears to be extraneous. If, on the other hand, DoD still intends to allow the contracting officer to grant approval for release, it should reinsert the language from the current version of DFARS 252.204-7000 in this regard.

D. **The Section Recommends That DoD Modify The Proposed Rule To Provide Additional Legal Protections To Contractors That Have Suffered A Cyber Incident**

1. The Rule Should Explicitly Provide a “Safe Harbor” in the Event of a Reported Incident

In its May 3, 2010 comments regarding the ANPR, the Section expressed concern that “by reporting a cyber intrusion, a contractor is increasing its risk of being found noncompliant with contract requirements.” We further commented that “[s]hould 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.” We note that the Proposed Rule takes a positive step forward by referencing, in the enhanced safeguarding context, NIST Special Publication (SP) 800-53 regarding “Recommended Security Controls for Federal Information Systems and Organizations.” We suggest that the Proposed Rule would be further improved by clarifying whether or to what extent a contractor’s adherence to the specified NIST controls would constitute a “safe harbor” in the event of a cyber intrusion. In addition, the Proposed Rule should clarify whether or
to what extent a contractor that provides the written determination described in 252.204–70YY(d)(2) after electing not to implement NIST controls could also take advantage of a “safe harbor.” Given the “other requirements” referenced in 252.204–70YY(e), the Section recommends a more detailed description of whether and to what extent a safe harbor may exist for contractors that adhere to the rule’s requirements but nevertheless experience a cyber incident.

In addition, we expressed a concern in our May 3, 2010, comments on the ANPR that “the necessary actions described in the ANPR are not sufficiently specific to serve as contract clause requirements.” Although this Proposed Rule addresses many of our prior concerns in the enhanced safeguarding context, we renew our concern as it relates to the basic safeguarding context. The Section also renews its suggestion that contractors that make cyber intrusion reports be offered a safe harbor, whether the contractor employs enhanced safeguarding controls or basic safeguarding controls.

2. The Section Recommends that DoD Revise the Cyber Intrusion Reporting and Investigation Cooperation Portions of the Proposed Rule

DFARS 252.204-70YY, addressing the enhanced safeguarding of unclassified DoD Information, calls for the reporting of cyber incidents within 72 hours of discovery of any cyber incident. See DFARS 252.204-70YY(f). Subsection (f)(2) requires reporting not only in the event of possible data exfiltration, manipulation, or loss of any DoD Information but also any time unauthorized access occurs on an unclassified system on which such data is residing or transiting. DFARS 252.204-70YY(f)(2). Subsection (5) sets forth a contractor’s responsibilities with respect to a reported cyber incident, including identifying, preserving, and protecting “images of known affected information systems and all relevant monitoring/packet capture data until DoD has received the image and completes its analysis, or declines interest” and cooperating with the DoD Damage Assessment Management Office (“DAMO”). DFARS 252.204-70YY(f)(5)(ii)-(iv). Subsection (6) of the proposed clause contemplates that DAMO may conduct a damage assessment and shall provide notice to the contractor to provide digital media. That same subsection states “the Contractor shall comply with DAMO information requests.” DFARS 252.204-70YY(f)(6).

Subsection (f)(2) of proposed clause 252.204-70YY(f) appears to be missing a section or to be incorrectly numbered in that subsection (f)(2)(ii) refers to incidents “not included in paragraph (f)(2)(i) or (ii).” Likewise, the contents of subsection (d) of 252.204-70YY appear to be incorrectly numbered. Specifically, the text currently denominated subdivision (d)(1) seems to constitute an introduction to the subdivisions of subsection (d) rather than the first of four coequal subdivisions. If this reading is correct, that introductory text should fall under subsection (d) and current subdivision (d)(2) should be relabeled (d)(1) and the other subdivisions adjusted accordingly.
Neither proposed Subpart 204.7400 nor DFARS 252.204-70YY sets forth criteria defining the circumstances under which DAMO may conduct a damage assessment, request digital media, including images of affected systems, from a contractor or otherwise restrict DAMO’s access in this area. We recommend that the proposed Subpart or clause delineate the Government’s specific obligations in a separate section. We recommend that, at a minimum, DoD modify the Proposed Rule to set forth clear and objective criteria under which DAMO may conduct an independent damage assessment or request digital media from a contractor. The Section believes that these government rights should be limited to cyber incidents involving actual data exfiltration or loss, and not incidents involving unauthorized access to a system on which information is resident or transiting where no data is extracted or lost.

Although the proposed clause requires a contractor to comply with all information requests, a contractor’s ability to provide the Government complete and unredacted access to digital media and images of affected systems is also impacted by the content of the data on those systems. An affected system is likely to contain a wide array of data other than unclassified DoD Information, including, but not limited to, personally identifiable information, other types of personal information, attorney-client privileged information, information subject to disclosure restrictions under federal, state, or international laws, or information subject to third party confidentiality protections. A contractor may not always be in a position to share such information as a result of other contractual or legal obligations.

DFARS 252.204-70YY specifically addresses the issue of third party information only. In pertinent part, the proposed clause states as follows:

(i) Third party information. If providing or sharing information is barred by the terms of a nondisclosure agreement with a third party, the Contractor will seek written permission from the owner of any third-party data believed to be contained in images or media that may be shared with the Government. Absent the written permission, the third-party information owner may have the right to pursue legal action against the Contractor (or its subcontractors) with access to the nonpublic information for breach or unauthorized disclosure.

Although the second sentence of the clause recognizes that contractors could face contractual liabilities for voluntarily producing such data, the clause, read as a whole, nevertheless appears to suggest that the contractor will need to produce such data in response to DAMO requests to comply with its contracts.

Because of other contractual or legal obligations and existing legal protections, we recommend that the Proposed Rule encourage the contractor to provide such digital media and images to the extent feasible. In cases where the
contractor does not share complete images with the Government due to legal, contractual, or other considerations, the Government has the right to avail itself of its options to legally compel the production of such digital media or images.

Rather than defining the scope of required information sharing by rule, the Section suggests that DoD rely on its currently available powers to compel production of information. These procedures have been established to protect all interested parties’ rights and interests and to ensure consistency with current state, federal, and international laws.

E. The Section Recommends That DoD Reconsider The Technical Requirements Of DFARS 252.204-70YY

The Section recommends that DoD reconsider the enhanced safeguards found in Table 1 under DFARS 252.204-70YY and whether those requirements can feasibly be implemented by large and small contractors alike. Although many businesses will have most of the requirements in place, the requirement to implement AU-10(5) and SC-13(4) appears to be different. Our understanding is that this requirement means that each company subject to this clause will have to implement a CAC, like a PKI system, on their unclassified networks. This could be a significant change for some contractors’ methods of securing unclassified data, as well as a costly and time consuming change. If DoD intends to require its contractors to upgrade their systems to require a comprehensive PKI system, then the Proposed Rule should state this intent more explicitly, recognize the cost and schedule implications, and revise the clause to accommodate the cost and schedule impact of this new requirement by requests for equitable adjustment. Alternatively, if DoD does not intend to require a CAC-like PKI system for DoD contractors, Table 1 should be revised to reflect this position.

II. CONCLUSION

The Section commends DoD’s use of the notice and comment process and its improvements to the Proposed Rule from the ANPR. These comments are meant to suggest additional improvements to 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 any final rule to address safeguarding of certain unclassified information. Specifically, the Section hopes that DoD will consider narrowing the scope of the Proposed Rule; clarify important definitions; delineate the parties’ respective roles and responsibilities under the Proposed Rule; consider the need for additional legal protections provided to parties that suffer cyber incidents; and examine the technical burdens the rule may impose on contractors. Finally, the Section suggests that once an interim or final rule is released, DoD provide a Frequently Asked Questions document or conduct a Question and Answer session with industry to provide answers to any questions that may remain.
The Section is available to provide additional information and assistance as DoD may require.

Sincerely,

Carol N. Park-Conroy
Chair, Section Public Contract Law

cc:
Mark D. Colley
Sharon L. Larkin
Stuart B. Nibley
David G. Ehrhart
Allan J. Joseph
John S. Pachter
Donald G. Featherstun
Council Members, Section of Public Contract Law
Co-Chairs, Cybersecurity, Privacy and Data Protection Committee
Kara M. Sacilotto