April 28, 2014

VIA REGULATORY PORTAL

General Services Administration
Regulatory Secretariat Division (MVCB)
ATTN: Hada Flowers
1800 F Street, NW, 2nd Floor
Washington, DC 20405

RE: Notice-OMA-2014-01; Docket No. 2014-0002; Sequence 8

Dear Ms. Flowers:

On behalf of the Section of Public Contract Law of the American Bar Association (“the Section”), I am submitting these comments to the Department of Defense (”DoD”) and General Services Administration (“GSA”) Joint Working Group on Improving Cybersecurity and Resilience through Acquisition.1 The Section consists of attorneys and associated professionals in private practice, industry, and Government service. The Section’s governing Council and substantive committees contain 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 have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and, therefore, should not be construed as representing the policy of the American Bar Association.2

1 Sharon L. Larkin, Section Chair, Mary Ellen Coster Williams, Section Delegate to the ABA House of Delegates, Jeri K. Somers, Budget and Finance Officer, and Candida Steel and Anthony N. Palladino, members of the Section Council, did not participate in the Section’s consideration of these comments and abstained from the voting to approve and send this letter.

2 Although these views are being presented on behalf of the Section only, they are generally consistent with the five guiding principles on cybersecurity that were developed by the ABA Cybersecurity Legal Task Force and adopted by the ABA Board of Governors in November 2012. The resolution setting forth these principles and other information regarding the Task Force’s mission and activities are available at: http://www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity.html.
These comments provide the Section’s perspectives on the key issues raised in the Joint Working Group’s Draft Implementation Plan, which seeks to translate the recommendations contained in the Joint Working Group’s Final Report on Improving Cybersecurity and Resilience through Acquisition (“the Report”) into “on-the-ground actions that will improve cybersecurity and resilience by reforming management of the people, processes, and technology involved in Federal Acquisitions.” The request for comments seeks stakeholder input on one of the six recommendations included in the Report. Specifically, the request seeks comments on the recommendation to “institute a federal acquisition cyber risk management strategy.” Among other things, the request seeks comments on whether the Implementation Plan for this recommendation provides a workable approach, whether the Plan development process provides adequate and appropriate opportunities for stakeholder input, what additional assumptions, clarifications, or constraints should be included in the Plan, whether the approach is adequate to achieve its goals, whether the major tasks and sub tasks in the plan are appropriate, and whether the definitions and taxonomy in Appendix I to the plan can be used to develop Overlays.

The Section applauds the Joint Working Group on its efforts to date in developing the Final Report and the Draft Implementation Plan as well as its efforts to seek out stakeholder input throughout this process. The Section further appreciates the Draft Implementation Plan’s reiteration of the Government’s ongoing commitment “to continuing the open, collaborative, stakeholder-centric process used to develop the recommendations in development of this Plan.” The Section urges the Joint Working Group to continue to seek out comments and stakeholder input and to do so in an even more fulsome manner that will allow on-going give and take between the Joint Working Group and the stakeholders. Specifically, the Section believes that workshops in the nature of those the National Institute of Standards and Technology (“NIST”) used as it developed the Cybersecurity Framework would be highly beneficial to both the Joint

---

3 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.”

4 The Implementation Plan adopts the definition of Overlays contained in NIST Special Publication 800-53, Rev. 4. That publication defines an Overlay as “A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.” In addition, the Implementation Plan states that each Overlay will include “1 An articulation of the level of risk presented by the Category …; 2. A specific set of minimum controls that must be included in the technical specifications, acquisition plan, and during contract administration and performance for any acquisition in the Category; 3. The universe of additional controls that are relevant to the Category but are not required in the minimum (i.e., a “menu”), and 4. Examples of sets of the identified additional controls that apply to particular use cases (e.g., FIPS 199 High or Moderate system acquisition), as applicable.” Draft Implementation Plan at 7.

5 Draft Implementation Plan at 3.

In addition, the Section recommends that the Joint Working Group seek a more holistic approach to implementing the recommendations contained in the Report – rather than implementing one recommendation at a time, cybersecurity and resilience may be better strengthened by implementing a number of the recommendations in a simultaneous, step-by-step manner. Finally, after reviewing the Implementation Plan and Appendix I, the Section was left with a number of questions that it feels should be answered or clarified in subsequent drafts of the Implementation Plan to ensure that all parties have a true understanding of the goals, steps, and responsibilities set out in the Implementation Plan.

I. Implementation of Many of the Report’s Recommendations Should be Done Simultaneously Instead of One Recommendation at a Time.

The final report of the DoD-GSA Joint Working Group on Improving Cybersecurity and Resilience through Acquisition released on January 23, 2014 recommended six important strategic reforms: (i) baseline cybersecurity requirements for selected acquisitions; (ii) cybersecurity training; (iii) common cybersecurity definitions; (iv) a federal acquisition cyber risk management strategy; (v) purchases from original equipment manufacturers, authorized resellers, or other trusted sources for selected acquisitions; and (vi) Government accountability for cyber risk management. Although the Draft Implementation Plan indicates that “[t]he Plan will be developed using an iterative process to facilitate sequential and concurrent implementation of the recommendations as appropriate,”6 the current draft document focuses exclusively on one recommendation – Institute a Federal Acquisition Cyber Risk Management Strategy. The Draft Implementation Plan explains this singular focus by stating that “the risk management strategy and processes to institute it provide the foundation that is necessary for the other recommendations to be implemented.”7 Although the Section certainly understands the desire and practical need to streamline the Joint Working Group’s early efforts, we recommend that the Joint Working Group consider expanding beyond that single recommendation in the early stages of this effort. The Section concurs that sequencing efforts and, more particularly, focusing on strategy early makes practical sense but also believes that the development of an effective cyber risk management strategy recommendation could benefit from incremental progress on other recommendations, particularly developing common cybersecurity definitions and improving cybersecurity training for Government personnel. The Section recommends that the Joint Working Group consider adopting a broader, more holistic approach

6 Id.
7 Id.
where synergies and incremental progress could be achieved across multiple recommendations.

II. Questions Remain Concerning the Draft Implementation Plan and Appendix I.

The Section believes that the Draft Implementation Plan provides a good start for implementing the recommendations in the Report. As a general matter, the Section cautions the Joint Working Group from attempting to establish a one-size-fits-all approach. Instead, the Section thinks general principles, guidelines, and strategies should be developed that companies will be able to utilize within their individual cybersecurity schemes.

The Section is also concerned that an overly specific set of overlays, especially one that uses product service codes as a means of determining which overlays will apply, will result in far more overlays than would be required or reasonably useful. That is, if different sets of security controls (i.e., different Overlays) will be utilized for each product or service procured by the government, the system will be overly complicated and could result in inconsistent requirements. This may take the form of inconsistency in the overlays themselves, for example if two or more products or services are procured in the same solicitation requiring an equal number of Overlays, or there is a risk of inconsistent security requirements and controls between the required overlays and other cybersecurity rules or regulations governing government contractors. For example, contractors competing for contracts on which Unclassified Controlled Technical Information may be used or distributed will already be subject to the NIST security controls in DFARS 252.204-7012. Other agencies can and often do impose additional, differing cyber security requirements as well.

Requiring the use of product-specific overlays in addition to the security controls that are already required is likely to result in additional cost and confusion to the contractors, without much if any additional security. The Section, thus, believes that a more general approach that will take into account the overlapping cyber risk concerns of a variety of products and services, as well as the obligations that contractors are already under is a better approach to ensure that there are no gaps in cyber security coverage, rather than attempting to apply a very specific set of security controls to each product or service procured.

In addition, our review of the current draft documents produced a number of questions that the Section believes should be answered, clarified, or considered in future drafts. Although we recognize that certain of these questions are at a level of detail that the Joint Working Group may not yet have had the opportunity to consider, our hope is that certain of these more detailed questions will be considered so as to assist the Working Group in better understanding operational concerns that may arise concerning the Draft. We have provided those questions below:
Determination of Cyber Risk:

1. Who makes the determination whether an item presents a security risk, and what are the guidelines for doing so?

2. When the implementation plan speaks of cyber risk, is it referring to all potential categories of risk (e.g., internal systems, internal threats, and external threats)?

3. To what extent will DoD or GSA provide assistance to agencies in developing both the threat and vulnerability aspects of the cyber risk assessments?

4. Given that the cyber risk profiles of the acquiring agencies play a role in determining the cyber risk of the contracting companies, what agency-level cyber risk assessments will be provided to prospective bidders prior to submitting proposals?
   a. Will cyber risk profiles be provided for the duration of the contract?

Categorization and Prioritization:

5. To what category level does the plan intend to apply overlays --the broad category (e.g., “hardware”), a subcategory (e.g., “peripherals and storage”), or an even smaller subset (e.g., “printer”)?
   a. What is the thought process behind the level to which the overlays will apply?

6. Will the implementation plan take into consideration the end user and/or anticipated use when prioritizing items?
   a. The Draft Implementation Plan currently recognizes that “the risk [an] item presents varies greatly according to the specific end user, often because of differences in the sensitivity of data sent to the device and the network it is connected to.” Nonetheless, the current method of prioritization envisioned by the implementation plan does not appear to take end use into account, and only prioritizes categories against each other.

7. Why does the implementation plan only prioritize categories against each other, and how will this be done?

8. Is it GSA’s vision that a contractor who produces multiple different products or provides many different categories of services would be subject to an wide variety of of enterprise-wide requirements as a result of its varied product-lines?

Overlays:

9. What types of “minimum security controls” does the implementation plan envision? From where will the security controls be derived? NIST SP 800-53? Commercial standards? Less specific security requirements, such as those in the Proposed FAR Rule (“best security available”)?

10. Why does the implementation plan contemplate “a universe of additional controls” in addition to the proposed required minimum controls?
a. What is the purpose, and who will decide when these additional controls are necessary? It appears this determination would be on a per procurement basis. If these additional controls are required when the risk of the procurement is higher, then shouldn’t this be part of step one (articulating the risk level)? Given the Draft Implementation Plan’s acknowledgement that risks change overtime and that Overlays may need to be updated on a regular basis (see Draft Implementation Plan at 7), will any changes to the Overlays relating to already-awarded contracts be changed by modification to the Contract?

11. What is meant by “sets of the identified controls that apply to particular use cases” (step four)? When would this be applicable, and what is the difference between step three and this step?

12. Who will ultimately develop the overlays? The draft implementation plan strives to create a repeatable methodology - does this mean overlays will be determined within each agency or be consistent throughout the Government?

13. How many different potential overlays does GSA contemplate creating?

14. Do you envision that the overlays will impose both enterprise-wide and product-specific requirements on contractor systems?

15. How prescriptive do you contemplate making the overlays?

16. Has GSA considered developing a set of guiding principles for how these overlays will be applied?

17. How does GSA anticipate applying these overlays to acquisitions for services?

18. What, within the NIST Framework, should serve as “a starting point for development of the requirements” for overlays for “appropriately defined categories of similar types.” (page iv of Appendix I)? How will the plan ensure the separate overlays for the Federal Risk and Authorization Management Program, Information Systems and Security Line of Business, and Federal Supply Schedule, do not lead to confusion and less uniformity?

19. How does GSA anticipate rolling out training on these categories and overlays to ensure a reasoned application and determination of the agency’s requirements?

**Annual Spend:**

20. What is the purpose of analyzing annual spend beyond determining what items the Government procures?
   a. Will annual spend will be used to determine cyber risk? An item that is more expensive is not necessarily riskier.

**Harmonization:**

21. How will the outputs of the draft implementation plan be harmonized with other, similar rules requiring security minimums (e.g., DoD Unclassified Controlled Technical Information Rule, DoDI 8510.01)?
22. What is the relationship between this initiative and the Proposed FAR rule on basic safeguarding of information systems?

Implementation:

23. How will the outputs of the implementation plan be implemented?
   a. Implementation through rulemakings? Agency FAR supplements?
24. Will there be exceptions? If so, for what and for whom?
25. Will it be possible to waive the requirements? If so, who determines whether there should be a waiver and will there be guidelines for doing so?
26. What will the process be when new technologies are developed or other uncategorized items need to be purchased? Who will be responsible for categorizing these items?
27. Will the implementation plan or any aspects of the cyber risk evaluations be considered controlled but unclassified? (If so, will they be subject to the updated DFARS requirements covering unclassified controlled technical information?)

III. Conclusion

The Section appreciates the opportunity to provide these comments and questions on the Draft Implementation Plan. We are available to provide additional information or assistance as you may require.

Sincerely,

Stuart B. Nibley
Chair-Elect, Section of Public Contract Law

cc: Sharon L. Larkin
    David G. Ehrhart
    James A. Hughes
    Jeri Kaylene Somers
    Council Members, Section of Public Contract Law
    Cybersecurity, Privacy and Data Protection Committee
    Kara M. Sacilotto
    Craig Smith