March 30, 2017

Via Regulations.gov

Department of Homeland Security
Office of the Chief Procurement Officer
Acquisition Policy and Legislation
ATTN: Ms. Candace Lightfoot
245 Murray Drive, Bldg. 410 (RDS)
Washington, DC 20528

Re: Homeland Security Acquisition Regulation (HSAR) Privacy Training

Dear Ms. Lightfoot:

On behalf of the American Bar Association (“ABA”) Section of Public Contract Law (“Section”), I am submitting comments on the Proposed Rule cited above. 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 Section is authorized to submit comments on acquisition regulations under special authority granted by the ABA’s Board of Governors. 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.

1 Mary Ellen Coster Williams, Section Delegate to the ABA House of Delegates, and Marian Blank Horn, Kristine B. 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

The Section understands both the need for, and importance of, privacy training for contractor employees who have access to Personally Identifiable Information (“PII”) in performing contracts for the Department of Homeland Security (“DHS”). We applaud DHS’s issuance of the Proposed Rule to amend the Homeland Security Acquisition Regulation Supplement (“HSAR”) to add a new subpart and contract clause to standardize the privacy training requirements throughout DHS. The Section supports this effort to ensure the proper handling and protection of PII under the Privacy Act of 1974.

The Section also supports DHS’s making available on a public website a DHS-developed privacy training module that contractors can provide to their employees to achieve compliance with the proposed requirements. This training enables contractors, particularly smaller businesses, to avoid incurring additional costs and expending resources to develop their own training. The Section believes, however, that certain contractors may desire to develop their own internal Privacy Act training that would be compatible with DHS’s rules and their own corporate policies, procedures, and training. The Section believes this preference may be particularly acute given the recently promulgated Federal Acquisition Regulation (“FAR”) privacy training requirement. The Section therefore requests that DHS implement a process by which contractors may obtain DHS approval for alternative privacy training.

In addition to DHS’s offering flexibility for training content, the Section recommends that DHS consider additional changes to the Proposed Rule described below. Adopting the Section’s proposed changes would provide more flexibility in how contractors meet the training requirement without adversely affecting DHS’s overall privacy objectives. The Section believes that the recommended changes would also facilitate contractors’ understanding of the requirements and, thus, improve compliance. Finally, these changes, if adopted, should ensure that DHS bears the privacy training costs only for contractor employees who actually handle PII or otherwise perform covered work involving systems of records.

II. COMMENTS

1. The Section Recommends Clarifying the Privacy Training Requirement’s Application by Incorporating the Statutory Definition of “System of Records.”

Under the Proposed Rule, the proposed clause HSAR 3052.224-7X, Privacy Training, would be included in all solicitations and contracts in which contractor and subcontractor employees may (i) have access to a Government system of records; (ii) handle PII or Sensitive Personally Identifiable Information (“SPII”); or (iii) design, develop, maintain, or operate a system of records on behalf of the Government. HSAR 3024.7004.

The Proposed Rule defines key terms such as PII, SPII, and “handling” but does not define a “system of records.” The Privacy Act does define a “system of records,” however, as “a group

---

of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.” The Act further requires agencies to file a notice about each system of records in the Federal Register; each notice is called a “System of Records Notice,” or “SORN.” DHS maintains a website listing its SORNs at https://www.dhs.gov/system-records-notices-sorns.

The Section recommends that DHS add the Privacy Act’s definition of a “system of records” to the Proposed Rule. This addition will increase understanding by both government and contractor personnel about when the clause and the training are required. For example, if a system does not include any PII or SPII or if all such data were rendered anonymous, a contract involving the system should not trigger the privacy training requirement. If contractors were required to implement privacy training for systems that did not actually include PII or SPII, both contractors, and ultimately DHS, would incur unnecessary costs.

2. The Section Recommends Requiring Flowdown of HSAR 3052.224-7X Only to Subcontractors with a Statement of Work that Triggers the Training Requirement.

The proposed HSAR Privacy Training clause requires contractors to “insert the substance of this clause in all subcontracts and require subcontractors to include this clause in all lower-tier subcontracts.” See HSAR 3052.224-7X(c) (emphasis added). This flowdown requirement is unnecessarily broad because the proposed HSAR 3052.224-7X(a) requires training only those contractor/subcontractor employees who may (i) have access to a Government system of records; (ii) handle PII or SPII; or (iii) design, develop, maintain, or operate a system of records on behalf of the Government. See HSAR 3052.224-7X(a). Thus, there should not be any need to flow down the clause to a subcontractor if its performance will not involve the activities listed in -7X(a) of the clause.

The Section therefore recommends that DHS modify paragraph (c) of the clause to read as follows:

The Contractor shall insert the substance of this clause in all subcontracts when individuals working on the subcontract will be performing tasks that meet the criteria established in Section (a) above. The Contractor also shall require subcontractors to include this clause in lower-tier subcontracts when individuals working on the lower-tier subcontract will be performing tasks that meet the criteria established in Section (a) above.

By making this change, DHS would facilitate subcontract negotiations by eliminating an unnecessary flow down clause and clarifying that privacy training is not required if a subcontractor’s performance at any tier will not involve access to a system of records, handling PII/SPII, or generally engaging with a system of records on behalf of the Government.

4 5 U.S.C. § 552a(a)(5).
3. **The Section Recommends that DHS Further Clarify the Requirement to Maintain Training Certificates and Leverage Electronic Recordkeeping When Available.**

Under the Proposed Rule, contractors must train all covered employees either within 30 days of award or, for employees joining the program after award, before the employees access the information identified in HSAR 3052.224-7X(a), and annually thereafter. See HSAR 3052.224-7(b). The Proposed Rule further states:

The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer and/or Contracting Officer’s Representative (COR) via email notification not later than thirty days after contract award or assignment to the contract. Subsequent training requirements shall be submitted to the Contracting Officer and/or COR via email notification not later than October 31st of each year. The Contractor shall attach training certificates to the email notification and the email notification shall list all Contractor and subcontractor employees required to complete the training and state the required Privacy training has been completed for Contractor and subcontractor employees.

Based on the Section’s review of the cited DHS training website, covered contractor and subcontractor employees would need to print the certificates individually after completing the online DHS privacy training and then submit them to the designated contractor employee for transmittal to the contracting officer. The contractor would be responsible for ensuring that all certificates, from both its own and its subcontractors’ covered employees, are collected and submitted to DHS. Depending on the number of individuals covered, this paper-intensive process will take significantly longer than the half hour estimated in the Paperwork Reduction Act section of the Federal Register notice.

Accordingly, the Section encourages DHS to explore secure technological alternatives for verifying compliance. For example, the Section recommends that DHS modify the Proposed Rule to allow contractors to place DHS’s publicly-available privacy training on their internally or externally hosted corporate training systems. This alternative would allow contractors to monitor, track, and report on employees’ completion of the required training in a more efficient manner. If permitted, contractors could provide consolidated electronic confirmation of training instead of manually collecting and tracking individually printed certificates. Although not all contractors necessarily have these types of systems, allowing those contractors who do to leverage this technology would not only mitigate the public reporting burden but also save both contractor and government time and resources.

In addition, the Section notes that HSAR 3052.224-7X(b) does not specify whether or for how long a contractor must “maintain” training certificates after submitting them to DHS. Out of an abundance of caution, contractors could feel compelled to keep the initial and annual certifications for all of their employees and subcontractors’ employees for periods exceeding contract performance, up to and extending beyond contract closeout and audit periods. For some
contractors, DHS would eventually bear the cost of this record retention, with little added benefit. The added value of having contractors retain copies indefinitely would be small because DHS will have its own record of compliance from the contractor.

Because the training is conducted annually and the clause requires the timely submission of training documentation to DHS, the Section recommends that DHS modify the Proposed Rule to clarify whether older training certificates must be maintained after submittal and, if so, the Section recommends that DHS specifically identify the retention period. The Section recommends that the period not exceed two years after the completion of the training.

Finally, the Section recommends that DHS consider changing the annual October 31st deadline specified in HSAR 3052.224-70X(a) for submittal of the training certifications:

From: “shall be submitted to the Contracting Officer and/or COR via email notification not later than October 31st of each year.”

To: “shall be submitted to the Contracting Officer and/or COR via email notification not later than October 31st of each year unless October 31st falls on a Saturday, Sunday, Federal holiday, or other day on which the Federal government is closed, in which case the submission shall be due on the next business day.”

This change will make the deadline conform to other federal deadlines, which generally permit the extension to the next business day whenever the due date falls on a day the federal government is closed.

III. CONCLUSION

The Section appreciates the opportunity to provide these comments and is available to provide additional information or assistance as you may require.

Sincerely,

James A. Hughes
Chair, Section of Public Contract Law

cc:
Aaron P. Silberman
Kara M. Sacilotto
Linda Maramba
Jennifer L. Dauer
Council Members, Section of Public Contract Law
Chairs and Vice Chairs, Cybersecurity, Privacy, and Data Protection Committee
Craig Smith
Samantha S. Lee