Via Regulations.gov

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


Dear Ms. Duggans:

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. Kasselerk, 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 recognizes the Department of Homeland Security’s (“DHS”) interest in ensuring the protection of its information systems and controlled unclassified information (“CUI”). The Section nonetheless believes that the proposed rule’s application and requirements are ambiguous and overbroad in places, namely that the proposed rule: (A) is in tension with the federal-government wide efforts for safeguarding of CUI led by the National Archives and Records Administration (“NARA”); (B) imposes an amorphous “adequate security” obligation that is difficult to implement; (C) appears to impose an overly broad incident-reporting obligation that could be read to extend to non-federal information systems, creating an undue burden on contractors; and (D) imposes overly broad obligations to flow the clause down to subcontractors. The Section offers these comments to address its observations and concerns.

II. COMMENTS

A. The Section Recommends Harmonizing Any Required Information Safeguarding Controls with the NARA Rule and NIST SP 800-171.

The scope of the proposed rule presents two significant concerns. First, the proposed rule appears to impose safeguarding requirements on contractors’ internal systems that are more appropriate for federal information systems. The preamble states that the safeguarding requirements apply to any contractor handling CUI and does not limit those requirements to contractors handling CUI on federal information systems. 82 Fed. Reg. 6430-31. Second, in so expanding the scope of coverage, the proposed rule ignores the multi-year federal initiative to harmonize the safeguarding requirements imposed on contractor information systems where CUI transits, is processed, or resides. The Section recommends that DHS not extend the proposed rule in its current form to contractor information systems and, instead, ensure that any such application is consistent with federal government-wide initiatives to protect CUI. The Section recommends in particular that DHS use National Institute for Standards and Technology (“NIST”) Special Publication (“SP”) 800-171 and the NARA framework to define both the required security controls and the pertinent categories of information to be protected.

As drafted, the proposed rule is silent on application (if any) of the NIST SP 800-171 controls to contractors’ own information systems. Because NIST SP 800-171’s purpose is to apply across the Government to contractors’ internal information systems, and because many companies are making significant investments to achieve compliance with this standard, the Section recommends that DHS clarify how SP 800-171’s controls fit with DHS’s requirements for “adequate security” for contractor internal systems. Such controls have been designated by NIST specifically for contractors’ internal systems and are preferable to internal agency guidance that may be intended solely for federal information systems. Indeed, NIST SP 800-171 was intended to remove the federal references and focus on a performance-based set of requirements that would be more easily applied to contractor information systems. The proposed rule thus seems incongruous with this larger, federal government-wide initiative.

In addition to overlooking this more standardized set of non-federal controls, the proposed rule also appears to create additional categories of CUI not currently contemplated
under the NARA regime. Of the twelve categories of information listed in the proposed rule’s definition of CUI, only eight are listed in the NARA Registry. Creating these new categories runs counter to the intended purpose of the NARA CUI Registry and associated rule, which expressly states that “agencies may use only those categories or subcategories approved by” the NARA Executive agent, as “published in the CUI Registry.” 32 C.F.R. § 2002.12(b). The Section recommends that DHS evaluate the NARA CUI Registry effort to consider whether that initiative will enable DHS to achieve its objectives.

Finally, as explained below, the current standards cited in the proposed clause are unclear and do not provide adequate guidance to contractors. In light of the concerns expressed in our comments, we believe the most efficient path would be to pause the ultimate implementation of the contractor information systems aspects of this rule to ensure alignment with the forthcoming FAR case contemplated under the NARA rule.

B. If DHS Declines to Adopt the NARA/ NIST SP 800-171 Regime, the Section Recommends Clarifying the Proposed Rule’s “Adequate Security” Requirement.

As drafted, the proposed HSAR 3052.204-7X(b) clause requires contractors to protect CUI resident on their own internal information systems by complying with DHS policies and procedures in effect at the time of award, and limiting contractors’ use, storage, and transmittal of CUI. Yet the cited website identifies several DHS-focused information security procedures that do not appear readily applicable to a contractor’s non-federal information systems. It is also unclear which requirements DHS believes apply to non-federal information systems.

As noted above, it was this uncertainty as to how internal, government-focused documentation applies to contractor information systems that led NARA and NIST to craft the separate NIST SP 800-171 guidance. The proposed rule appears to retreat from the NIST effort to bridge this gap between government and contractor systems. In doing so, the proposed rule does not provide sufficient guidance on what controls contractors must implement to comply with the proposed rule itself.

Accordingly, if DHS continues implementing its own, agency-specific paradigm despite the considerations presented above, the Section offers the following recommendations for revising the proposed rule. Although the Section applauds the Agency’s decision to use a risk-based assessment for determining whether the contractor’s security measures are “adequate” under the new clause, see HSAR 3052.204-7X(a)-(b), we believe that not citing controls applicable to contractors could lead to inconsistent and potentially uncertain implementation and enforcement results. Therefore, the Section recommends that DHS consider the following suggestions as it proceeds with the rulemaking process:

- The Section recommends specifying whether DHS intends to be the arbiter of compliance or if contractor self-assessments will suffice—which the Section recommends.

If DHS intends to serve as the arbiter of whether the contractor has implemented “adequate security” as required by the proposed clause, we recommend the proposed rule clarify how any determination of adequacy will be made. We suggest that this authority be placed at a level higher than the contracting officer, such as the chief information officer (“CIO”), to ensure a more uniform application across DHS. We also recommend that DHS include further guidance on this subject on the cited website to explain to contractors how this standard will be applied.

- Second, the Section recommends that DHS establish mechanisms through which contractors can obtain sufficient clarity during the proposal stage both to determine whether CUI will be processed under the contract and, if yes, to assess whether they can comply with such safeguarding obligations.

- Third, we recommend that DHS consider implementing a review process for ensuring that contractors can propose alternative, but equally effective, controls akin to those in the Department of Defense information-safeguarding rule. We recommend that the process also include a procedure through which contractors can obtain confirmation that a particular control is unnecessary. We suggest that the final rule clarify the process for making such determinations and recommend that contractors be permitted to make such determinations on an individual basis.

C. The Section Recommends Narrowing the Incident Reporting Obligation.

The proposed rule imposes broad reporting obligations that exceed the scope of similar contractor reporting obligations. The proposed rule requires reporting “all known or suspected incidents.” HSAR 3052.204-7X(d). An “incident,” as defined in the proposed rule, includes the breach of any “information system,” including contractor information systems. See HSAR 3052.204-7X(a). Under the proposed rule, there are separate definitions for a “federal information system” and “information system,” and the incident reporting obligation does not limit the scope of reportable incidents to federal information systems or even contractor information systems that contain federal information. See id. Thus, the proposed rule could be read to require a contractor to report to DHS any incident impacting its own internal information systems, regardless of whether the incident has any likelihood of impacting the DHS CUI resident on that information system.

This proposed rule could impose a wider reporting requirement than any of the current safeguarding regulations. Although the Section recognizes DHS’s desire to obtain information regarding all actual and potential unauthorized disclosure of DHS CUI, the Section nevertheless believes this reporting obligation can be tailored to reduce the administrative burden that the proposed rule appears to impose upon DHS contractors. To that end, the Section once again suggests that DHS harmonize its efforts in this area with any reporting obligations currently under consideration by the FAR Council in conjunction with its federal government-wide application of the NARA Rule to federal contractors.
Moreover, the combination of the broad reporting requirement and the one-hour reporting timeline for “all known or suspected incidents involving [Personally Identifiable Information ("PII") or [Sensitive Personally Identifiable Information ("SPII")],” along with the requirement that contractors report all “suspected” incidents, may result in the reporting of a substantial number of “false positives.” Such a result would be unduly burdensome for both contractors and DHS alike. To limit reporting of “suspected” incidents that are ultimately found after review to not present an intrusion, the Section recommends extending the reporting timeframes to eight hours for known incidents and 72 hours for suspected incidents involving contractors’ internal information systems.

On a similar note, the Section requests that DHS consider extending the five-day notification requirement to affected individuals to enable contractors to dedicate resources to remediation and investigation activities in the initial days after a breach. The five-day notification period is substantially shorter than most state reporting obligation (30-45 days in many states). Many companies reflect these state time periods for providing notifications to affected individuals. The Section is concerned that the notification timeline will detract from contractors’ ability to meaningfully respond to the incident.

D. The Mandatory Flowdown Requirement Should Apply Only When Contractors Will Have Access to CUI or Covered Information Systems.

The proposed clause mandates that “[t]he Contractor [shall] insert [the substance of] this clause in all subcontracts and require subcontractors to include this clause in all lower-tier subcontracts.” See HSAR 3052.204-7X(j) (emphasis added). The Section believes that this flowdown requirement is unnecessarily broad because it would require flowdown to a subcontractor even if its employees will have no access to DHS systems or information resources or even DHS CUI. The Section maintains that there is no need to flow down the clause to a subcontractor if none of its employees will have such access.

The Section therefore recommends that DHS modify section (j) to read:

The Contractor shall insert the substance of this clause in all subcontracts when the subcontractor’s employees will have access to systems identified above and require subcontractors to include this clause in lower-tier subcontracts when the lower-tier subcontractor’s employees will have access to systems identified above.

By making this change, DHS would facilitate subcontract negotiations by eliminating an unnecessary flowdown clause and clarifying that such safeguarding is not required if a subcontractor’s performance at any tier will not involve access to such systems.
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