

2016-2017

**CHAIR**

James A. Hughes  
3734 N Woodrow St  
Arlington, VA 22207  
(571) 382-0700

**CHAIR-ELECT**

Aaron P. Silberman  
311 California St, 10th Floor  
San Francisco, CA 94104  
(415) 956-2828

**VICE-CHAIR**

Kara M. Sacilotto  
1776 K St, NW  
Washington, DC 20006  
(202) 719-7107

**SECRETARY**

Linda Maramba  
2980 Fairview Park Dr  
Falls Church, VA 22042  
(703) 280-4086

**BUDGET AND FINANCE OFFICER**

Jennifer L. Daurer  
500 Capitol Mall, Ste 2200  
Sacramento, CA 95814  
(916) 492-5073

**SECTION DELEGATES**

Mary Ellen Coster Williams  
717 Madison Pl, NW, Ste 612  
Washington, DC 20005  
(202) 357-6660

Michael W. Mutek  
6645 Briar Ridge Lane  
Plano, TX 75024  
(214) 673-7197

**IMMEDIATE PAST CHAIR**

David G. Ehrhart  
Fort Worth, TX

**PREVIOUS PAST CHAIR**

Stuart B. Nibley  
Washington, DC

**COUNCIL MEMBERS**

Patricia Hale Becker  
McLean, VA

Justin M. Ganderson  
Washington, DC

Marian Blank Horn  
Chevy Chase, MD

Andrew D. Irwin  
Washington, DC

Kristine B. Kassekert  
Arlington, VA

John E. McCarthy, Jr.  
Washington, DC

Kevin P. Mullen  
Washington, DC

Bryant Gregory Snee  
Washington, DC

Robert J. Strauss  
Aurora, CO

Brian G. Walsh  
Washington, DC

Heather K. Weiner  
Washington, DC

Eric Whytsell  
Denver, CO

W. Hartmann Young  
Washington, DC

**EDITOR, PUBLIC CONTRACT**

**LAW JOURNAL**  
Patricia H. Wittie  
Washington, DC

**EDITOR, THE PROCUREMENT**  
**LAWYER**

Nicole Owen-Wiest  
Washington, DC

**BOARD OF GOVERNORS LIAISON**

William C. Carpenter, Jr.  
Wilmington, DE

**SECTION DIRECTOR**

Patricia A. Brennan  
321 N Clark St, M/S 19.1  
Chicago, IL 60654  
(312) 988-5623

**Writer's Address and Telephone**

James A. Hughes  
3734 N. Woodrow St.  
Arlington, VA 22207  
[ty@hugheslawplc.com](mailto:ty@hugheslawplc.com)

March 30, 2017

**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

**Re: Homeland Security Acquisition Regulation (HSAR); Information  
Technology Security Awareness Training (HSAR Case 2015-002), 82  
Fed. Reg. 6446 (Jan. 19, 2017)**

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.<sup>1</sup> 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.<sup>2</sup>

<sup>1</sup> 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.

<sup>2</sup> This letter is available in pdf format at [http://www.americanbar.org/groups/public\\_contract\\_law/resources/prior\\_section\\_comments.html](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, harmonized information-technology security-awareness training for contractor employees who have access to Department of Homeland (“DHS”) information systems and information resources. We applaud DHS’s efforts to standardize the applicable training requirements across DHS by issuing a Proposed Rule to amend the Homeland Security Acquisition Regulation Supplement (“HSAR”) to add a new subpart and contract clause. As discussed more fully below, the Section nevertheless recommends that DHS limit the application of the Proposed Rule to DHS information systems and information resources or those operated on its behalf—and not also including “contractor owned and/or operated systems capable of collecting, processing, storing or transmitting controlled unclassified information (“CUI”) under the contract.”

The Section also supports DHS’s making available on a public website DHS-developed training and Rules of Behavior (“RoBs”) to facilitate contractor compliance with the proposed requirements. This training enables contractors, particularly smaller businesses, to avoid incurring additional costs and expending resources to develop their own information-technology security-awareness training. The Section believes, however, that certain contractors may desire to develop their own customized training and/or user requirements so that contractor-specific information security controls and requirements can be added, as appropriate. The Section therefore requests that DHS implement a process by which contractors may obtain DHS’s approval for alternative information-technology awareness training initiatives.

In addition to DHS’s narrowing the application of the Proposed Rule and providing for flexibility as to training content, the Section recommends that DHS consider certain other additional modifications described below. Adopting the Section’s proposed changes would facilitate contractor understanding of the requirements, and thus improve compliance, without adversely affecting DHS’s information technology security objectives. Finally, these changes, if adopted, should ensure that DHS bears the training costs only for contractor employees who actually access the covered systems.

## **II. COMMENTS**

### **A. The Section Recommends Limiting the Proposed Rule’s Application.**

The Proposed Rule imposes two requirements on contractor and subcontractor employees who access certain information systems or information resources: (1) take initial and annual information technology security awareness training; and (2) sign DHS’s RoBs governing the use of DHS systems and resources that include sensitive information. HSAR 3052.239-7X(a) - (b). DHS asserts that these proposed changes “are necessary to ensure contractors and subcontractors understand their roles and responsibilities in ensuring the security of systems and the confidentiality, integrity and availability of CUI.” 82 Fed. Reg. at 6447.

Notably, the Proposed Rule applies not only to DHS’s information systems and information resources, but also to all “contractor-owned and/or operated information systems and resources capable of collecting, processing, storing or transmitting controlled unclassified (CUI)

information.” Proposed HSAR 3039.7001. The Proposed Rule defines “information resources” and “information systems” generically and thus does not limit application of the Proposed Rule to only those contractor-owned information systems and information resources operated on DHS’s behalf. *See* Proposed HSAR 3002.101. The Proposed Rule places only one express limitation on its application to contractor-owned and/or operated information systems or information resources: such systems must be “capable of collecting, processing, storing or transmitting” CUI. *E.g.*, Proposed HSAR 3039.7001 (scope), 3039.7003 (contract clause).

The Section finds this coverage to be too broad and in need of tailoring. In particular, almost *any* information system or information resource is “capable of collecting, processing, storing or transmitting” any type of data, CUI or otherwise. Even if the Proposed Rule were clarified to apply only to contractor-owned information systems and information resources that actually collect, process, store, or transmit CUI, the Section would still find the Proposed Rule to be ambiguous, overly broad and potentially inconsistent with Executive Order No. 13556, *Controlled Unclassified Information*,<sup>3</sup> for the following three reasons.

First, because the Proposed Rule does not reference the CUI Program administered by the National Archives and Records Administration (“NARA”), which is intended to standardize how Executive Branch agencies handle CUI, the Proposed Rule creates the potential for ambiguity and confusion. In September 2016, NARA issued a final rule that established the NARA CUI registry and associated agency requirements, including identification and marking of CUI.<sup>4</sup>

Nonetheless, in defining CUI, the Proposed Rule does not cite this regulation or the NARA CUI registry. Instead, the Proposed Rule defines CUI as:

[A]ny information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. Within the context of DHS, this includes such information which, if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy of individuals.

Proposed HSAR 3002.101. The Proposed Rule also identifies 12 specific categories and subcategories of information as included in the CUI definition. The Proposed Rule does not align these categories and subcategories with the categories and subcategories in the NARA CUI registry and associated requirements. The Section is thus concerned that the Proposed Rule will create confusion, will potentially undermine NARA’s government-wide CUI initiative, and will create the very type of agency-specific approach to managing CUI that Executive Order No. 13556 sought to eliminate.

---

<sup>3</sup> 75 Fed. Reg. 68675 (Nov. 9, 2010).

<sup>4</sup> 81 Fed. Reg. 63324 (Sept. 14, 2016).

Second, although the Proposed Rule appears to apply to contractors' internal computing systems that handle CUI, the Proposed Rule does not appear to account for National Institute for Standards and Technology ("NIST") Special Publication ("SP") 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. SP 800-171 was created specifically to establish uniform government-wide security requirements for nonfederal information systems that contain CUI and that are not operated on behalf of federal agencies. The Section has long advocated that, to the extent practical, federal agencies implement uniform, harmonized information security requirements on contractors' internal systems. The Section thus does not find it necessary for contractor and subcontractor employees to take training and sign RoBs focused on DHS security rules when those employees' only access is to internal company systems potentially (indeed, likely) subject to other federally mandated controls.

Third, many contractors have expended significant resources to implement extensive risk-based security controls based on DoD's or other agencies' imposing NIST SP 800-171 security controls or other industry standards. These contractors have developed policies and procedures around such controls and have trained their employees on the policies. Thus, based on their own risk assessments, contractors may be implementing more rigorous security controls or user requirements than the Proposed Rule would require. In addition, DHS's information technology security awareness training or RoBs may conflict with individual contractors' security requirements applicable to information systems or information sources that store or process other sensitive information along with DHS CUI. For example, the RoB currently posted online appears intended solely for use in connection with DHS systems and IT resources. The Section finds it impractical to require employees to sign such paperwork or to take DHS-specific training when those employees access only internal company information systems that are not operated on DHS's behalf.

Accordingly, the Section recommends that DHS modify the Proposed Rule by narrowing its application to DHS's information systems or information resources or those operated by a contractor on DHS's behalf.

**B. The Section Recommends Requiring Flowdown of HSAR 3052.239-7X Only to Subcontractors That Have Access to Covered Systems or Information Resources.**

The proposed clause HSAR 3052.239-7X, HSAR Information Technology Security Awareness Training, 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 3052.239-7X(c) (emphasis added). This flowdown requirement is unnecessarily broad. The provision would require flowdown to a subcontractor even if its employees will have no access to DHS's systems or information resources or even to DHS CUI. The Section believes it is unnecessary for prime contractors to flow down the clause to a subcontractor in these circumstances.

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 subcontracts when individuals working on the subcontract will have access to systems identified above and require subcontractors to include this clause in lower-tier subcontracts when individuals working on the lower-tier subcontract 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 the training and RoBs are not required if a subcontractor's performance at any tier will not involve access to such systems.

**C. The Section Recommends that DHS Further Clarify the Requirement to Maintain Training Certificates and RoBs and Leverage Electronic Recordkeeping When Available.**

Under the Proposed Rule, contractors must train all covered employees and have them sign RoBs either within 30 days of award or, for employees joining the program after award, before accessing the covered systems, and annually thereafter. *See* HSAR 3052.239-7X(a) - (b). The Proposed Rule further requires contractors to "maintain copies" of the associated training certificates and RoBs "for all Contractor and subcontractor employees as a record of compliance." *Id.* The documentation requirement is then set forth as follows:

[F]or 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 31<sup>st</sup> of each year.

HSAR 3052.239-7X(a). In addition to emailing the documentation, the contractor must identify all contractor and subcontractor employees required to complete the training and verify that all such individuals have been trained. *Id.*

Based on the Section's review of the DHS website cited in the Proposed Rule, covered contractor and subcontractor employees would need to print the certificates individually after completing the online DHS training, 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. *See* 82 Fed. Reg. at 6448.

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 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 completion 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 the Proposed Rule does not specify whether or for how long a contractor must "maintain" training certificates or RoBs after submitting them to DHS. Out of an abundance of caution, contractors could feel compelled to keep the initial and annual documentation 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 the older training documents 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 31 deadline specified in HSAR 3052.239-70X(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.

Ms. Shaundra Duggans

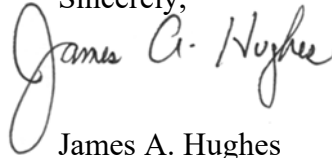
March 30, 2017

Page 7

### **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,

A handwritten signature in dark ink, reading "James A. Hughes". The signature is fluid and cursive, with the first name "James" being more prominent.

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