October 23, 2012

VIA REGULATORY PORTAL AND ELECTRONIC MAIL

General Services Administration, Regulatory Secretariat (MVCB)
ATTN: Hada Flowers
1275 First Street NE., 7th Floor
Washington, DC 20417


Dear Ms. Flowers:

On behalf of the Section of Public Contract Law of the American Bar Association (“the Section”), I am submitting comments on the above-referenced Proposed Rulemaking: FAR Case 2011-020; Basic Safeguarding of Contractor Information Systems, 77 Fed. Reg. 51496 (Aug. 24, 2012) (hereinafter “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 This letter is available in pdf format under the topic “Cybersecurity; Access to and Protection of Information” at: http://www.americanbar.org/groups/public_contract_law/resources/prior_section_comments.html.
Board of Governors of the American Bar Association and therefore should not be construed as representing the policy of the American Bar Association.²

The Section recognizes that federal agencies subject to the Federal Acquisition Regulation (“FAR”) have various directives and regulations that address the protection or release of unclassified information. The Section appreciates the efforts that the FAR Council has made with respect to this guidance. Furthermore, we commend the Council for its efforts on the Proposed Rule and for its consideration of prior comments, including those submitted by the Section, on the Department of Defense (“DoD”) Advance Notice of Proposed Rulemaking (“ANPR”) and notice of public meeting in the Federal Register, 75 Fed. Reg. 9563 (Mar. 3, 2010), under Defense Federal Acquisition Regulation Supplement (“DFARS”) Case 2008-D-028, Safeguarding Unclassified Information.

I. COMMENTS

The stated purpose of the Proposed Rule “is to improve the protection of information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems by employing basic security measures, as identified in the clause to appropriately protect information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems from unauthorized disclosure, loss, or compromise.” 77 Fed. Reg. 51497. As noted in our comments to the 2010 DoD ANPR, defining improvements to industry’s cybersecurity practices through regulation 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, on the one hand, and the significant costs in terms of adding security measures, on the other; (iii) contractors’ need to understand their contractual obligations at the time of award; and (iv) the reality that cybersecurity incidents are often difficult to prevent, even if a contractor maintains a high standard of security.

The Section’s comments address the following areas intended to improve the final rule: (1) the scope of the Proposed Rule; (2) clarifications to definitions; and (3) the roles and responsibilities of the parties.

² Jeri Kaylene Somers, a Section Officer, and Candida Steel, 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.
A. The Section Recommends Narrowing The Proposed Rule

1. The Section Recommends that the FAR Council Revise and Clarify the Description of Information Generated for the Government

The Proposed Rule covers “information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems.” 77 Fed. Reg. 51498; FAR 4.1700. Contractors produce a wide variety of “information . . . generated for the Government,” such as periodic reports, data items, database compilations, regulatory submissions, contract administration data, and offerors’ proposals, by way of example. Some of this information may be proprietary; some information is not; and some information may not be marked or identified as proprietary or non-proprietary.

To the extent that the Proposed Rule extends to a contractor’s proprietary information submitted to the Government, the Section recommends narrowing the Proposed Rule. The contractor should bear the responsibility for performing a risk-based assessment of contractor proprietary information, weighing the costs and benefits of security safeguards and deciding what serves as an appropriate level of protection based upon the value of the information, level of risk, and cost-effectiveness of security. Accordingly, the Section recommends clarifying the Proposed Rule to exclude contractor proprietary or trade secret data from the scope of “information . . . generated for the Government” so that the responsibility for safeguarding such information “resident on or transiting through the contractor information systems” remains with the contractor.

2. The Section Recommends that the FAR Council Revise and Clarify the Definition of “Public Information”

The Proposed Rule specifically excludes “public information” from the types of information contractors must safeguard. 77 Fed. Reg. 51498; FAR 4.1700. The Proposed Rule incorporates the definition from 44 U.S.C. § 3502 that defines public information as “any information regardless of form or format, that an agency discloses, disseminates, or makes available to the public.”

The Section is concerned that this proposed definition might be construed as limiting “public information” to such information that is already in the public domain. If so, the definition may be too narrow, as the Government has significant volumes of data that have not yet be made public, but that may be subject to obligations for disclosure under a variety of statutes. For example, the Freedom of Information Act (“FOIA”) generally establishes a policy of making federal
information available to the public. 5 U.S.C. § 552. Under FOIA, exceptions do exist, but the Federal agency must justify withholding requested information under one of the express statutory exemptions from disclosure, such as national defense or foreign policy secrets, confidential commercial or financial information, private personnel and medical files, certain law enforcement records, and other expressly enumerated exceptions under FOIA. 5 U.S.C. § 552(b).

Similarly, the e-Government Act of 2002 sets forth multiple legislative objectives for disseminating federal information publicly:

(5) To promote the use of the Internet and emerging technologies within and across Government agencies to provide citizen-centric Government information and services.

* * *

(8) To promote access to high quality Government information and services across multiple channels.

(9) To make the Federal Government more transparent and accountable.

* * *

(11) To provide enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy, national security, records retention, access for persons with disabilities and other relevant laws.

Pub. L. No. 107-374, § 2, 116 Stat. 2900 (2002). Accordingly, Federal agencies must consider these statutory policies in determining the public availability of information held by the Government or provided to contractors.

Consistent with these statutory policies for public disclosure and Government transparency, the Section recommends that the FAR Council clarify the Proposed Rule and narrow its scope to “publicly available” information consistent with applicable statutory requirements (including FOIA), rather than simply “public information.”
3. The Section Recommends that the FAR Council Revise and Clarify the Definition of “Best Level of Security and Privacy Available”

The proposed clause at 52.204-XX on the basic safeguarding of contractor information systems requires the transmittal of electronic information “using technology and processes that provide the best level of security and privacy available, given facilities, conditions, and environment.” 77 Fed. Reg. 51499; 52.204-XX(b)(2) (emphasis added). The stated purpose of the Proposed Rule, however, is to provide for “basic security measures,” rather than the “best level” of safeguards. 77 Fed. Reg. 51497.

In addition, the proposed “best level of security and privacy available” standard 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 the Federal Information Security Management Act (“FISMA”). Given the evolving nature of cybersecurity threats, new security technology and processes are constantly being developed and will continue to be developed. The constant evolution of security technology may impose a significant and unnecessary cost burden on contractors striving to achieve the undefined, and constantly changing, standard of “the best level of security and privacy available.”

Finally, the Section notes that this proposed standard may not be consistent with the cost-effectiveness standards and risk-based approach established by FISMA. See 44 U.S.C. § 3544(a)(2)(C) (“implementing policies and procedures to cost-effectively reduce risks to an acceptable level”). We believe that the level of security should be defined in conjunction with the cost-effectiveness standard established by FISMA. Accordingly, the Section recommends that the FAR Council replace the phrase “best level of security and privacy available” with the phrase “adequate security and privacy safeguards.”

4. The Section Recommends that the FAR Council Revise and Clarify the Restriction on Use of Public Computers

The Proposed Rule’s objective is “for the basic safeguarding of contractor information systems that contain information provided by or generated for the Government that will be resident on or transiting through contractor information systems.” 77 Fed. Reg. 51496. The Section recommends that the FAR Council revise Proposed Rule and associated FAR clause to focus on covered contractor information systems (as intended by the rule) instead of proscribing more generalized information protection standards that could have unintended
consequences. For example, the Proposed Rule currently includes the following potentially overbroad restrictions focusing on protecting information on public computers or web sites:

1. Protecting information on public computers or Web sites: **Do not process information** provided by or generated for the Government (other than public information) on public computers (e.g., those available for use by the general public in kiosks, hotel business centers) or computers that do not have access control. Information provided by or generated for the Government (other than public information) shall not be posted on Web sites that are publicly available or have access limited only by domain/Internet Protocol restriction. Such information may be posted to web pages that control access by user ID/password, user certificates, or other technical means, and that provide protection via use of security technologies. Access control may be provided by the intranet (versus the Web site itself or the application it hosts).

77 Fed. Reg. 51499; 52.204XX(b)(1) (italics in original) (bold added).

First, if the FAR Council determines that it will not focus exclusively on contractor systems and includes in a final rule a restriction regarding the use of “public computers” for non-public information provided by or generated for the Government, the Section recommends more clearly defining the term “public computers.” Currently, the Proposed Rule parenthetically references as examples of a “public computer” both a computer device (“kiosks”) and a location (“hotel business centers”); it does not, however, define the term. The Section recommends that, if the FAR Council retains this restriction, that it define “public computers” more narrowly as computers located in public areas that the general public may use for general purposes.

Second, the Section recommends that the Proposed Rule reflect that some contractors are contractually obligated under certain contracts to maintain and generate covered information on kiosks and other publically-accessible computers located in public places. For example, under the Transportation Security Administration’s Transportation Workers Identification Credential (“TWIC®”) program, individuals may enroll at contractor-managed enrollment computer stations at public locations such as shipping/mail retail stores, hotels, and colleges.
Placing restrictions on contractor use of “public” computers in performance of a contract may conflict with a contractor’s specific contractual obligations and an agency’s stated requirements. The Section recommends that the FAR Council modify the Proposed Rule to address this unintended consequence.

Third, the Section recommends that the FAR Council modify the Proposed Rule to remove the restriction on the use of public computers if the user has implemented a secure means of accessing the covered Government information so that it is reasonably protected from compromise. Many companies have established secure remote access capabilities that include identity authentication or other controls that reasonably protect against the risk of compromise. Therefore, the Section recommends that if this section of the Proposed Rule is retained, the FAR Council modify it to include exceptions in a manner similar to those for the web posting restriction in the clauses quoted above.

B. The Section Recommends that the FAR Council Clarify Other Definitions in the Proposed Rule

1. The Section Recommends Clarifying the Term “Safeguarding”

The Proposed Rule defines the term “Safeguarding” as “measures or controls that are prescribed to protect information.” 77 Fed. Reg. 51499; 52.204XX(a). This definition neither refers to nor incorporates the established definition of “information security.” For example, the FAR presently defines “information security” as follows:

“Information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
(3) Availability, which means ensuring timely and reliable access to, and use of, information.

FAR § 2.101; see also 44 U.S.C. § 3542(b)(1).

In this context, the Proposed Rule is not clear as to whether it draws a distinction between “safeguarding” and “information security.” If a distinction is intended, the Proposed Rule should be clarified in this regard. If “safeguarding” and “information security” have the same meaning and intent, the Section recommends that the FAR Council revise the Proposed Rule either to incorporate the definition of “information security” into meaning of “safeguarding” or to replace “safeguarding” with “information security.”

2. The Terms “Voice” and “Information” Should be Clarified

The Proposed Rule broadly defines the terms “information” and “voice.” The term “information” means “any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.” 77 Fed. Reg. 51499; 52.204XX(a). The term “voice” means “all oral information regardless of transmission protocol.” 77 Fed. Reg. 51499; 52.204XX(a). Later, the proposed clause combines the terms “voice” and “information” as follows:

Transmitting voice and fax information. Transmit information provided by or generated for the Government (other than public information), via voice and fax only when the sender has a reasonable assurance that access is limited to authorized recipients.

77 Fed. Reg. 51499; 52.204XX(b)(3) (italics in original).

Together, the terms “voice” and “information” could arguably apply to any oral communication, regardless of its transmission protocol, such as a telephone conversation. The Section recommends that the FAR Council clarify the scope of “voice information” in the Proposed Rule, including clarifying whether it applies to telephone conversations, digital audio recordings of oral information, digital transcripts of the same (e.g., voicemail message), or other voice-based communications.
C. The Section Recommends that the FAR Council Clarify the Roles and Responsibilities of the Parties Under the Proposed Rule

The Proposed Rule places limitations upon the transfer of information by a contractor to its subcontractors:

Transfer limitations. Transfer information provided by or generated for the Government (other than public information) only to those subcontractors that both require the information for purposes of contract performance and provide at least the same level of security as specified in this clause.

77 Fed. Reg. 51499; 52.204XX(b)(7) (italics in original).

The Section believes that the Proposed Rule is unclear regarding whether a party has any affirmative responsibility for reviewing or approving a subcontractor’s level of security. Many subcontractors perform work for more than one prime contractor, making it possible that a subcontractor will face different security standards requirements as well as conflicting interpretations of those requirements. Moreover, because the basic safeguarding requirements in the Proposed Rule are broadly worded, the Proposed Rule affords subcontractors with broad flexibility to comply. We believe that the Proposed Rule would be improved by focusing on the need for subcontractors to agree to meet the basic safeguarding requirements. Accordingly, the Section recommends revising the Proposed Rule to state that the transfer of information should be “only to those subcontractors that both require the information for purposes of contract performance and that agree to provide at least the same level of security as specified in this clause.”

In addition, contractors may need to provide non-public government information to subcontractors (and subcontractors may need access to such information) prior to the entry into a subcontract agreement. We assume that if non-public government information relating to contract performance needs to be exchanged, a prime contractor would flow down appropriate restrictions through a non-disclosure agreement or similar method that would impose appropriate safeguards, limit disclosure, and impose disposal requirements. Such a practice would be consistent with other safeguards that agencies and contractors generally apply to proprietary or trade secret data. Because of this potential pre-contract need for information exchange, the Section recommends that the FAR Council revise the above-referenced clause to apply to “information for purposes relating to a contract” instead of “information for purposes of contract performance.”
II. CONCLUSION

The Section commends the FAR Council’s use of the notice and comment process and its efforts to improve the Proposed Rule based upon input from prior proposed rules. These comments are meant to suggest additional improvements to the FAR Council’s implementation effort. The Section also encourages the FAR Council to continue to seek out the assistance of federal agencies and the public in the process of refining these proposed regulations. The Section respectfully requests that the FAR Council consider the issues identified in these comments in developing any final rule to address information security for certain unclassified information. Specifically, the Section believes that the final rule would be improved by narrowing its scope, clarifying important definitions, and delineating the parties’ respective rules and responsibilities under the Proposed Rule. Finally, the Section suggests that once an interim or final rule is released, the FAR Council 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 the FAR Council may require.

Sincerely,

Mark D. Colley
Chair, Section of Public Contract Law

cc:
Sharon L. Larkin
Stuart B. Nibley
David G. Ehrhart
Jeri Kaylene Somers
Council Members, Section of Public Contract Law
Chair(s) and Vice Chair(s) of Cybersecurity, Privacy and Data Protection Committee
Kara M. Sacilotto
Craig M. Smith