Dear Ms. Flowers:


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.² 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.³

¹ 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.”

² Jeri K. Somers, a Section Officer, and Candida S. Steel, a Council Member, did not participate in the Section’s consideration of these comments and abstained from the voting to approve and send this letter.

³ 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...
The RFI seeks information as to three primary areas - “Feasibility and Federal Acquisition,” “Commercial Practices,” and “Harmonization.” See 78 Fed. Reg. 27966-68. These comments address selected key issues within each of these areas. In general, we believe that the Working Group should incorporate the following principles in its final recommendations to the President: (1) that successful efforts to improve cybersecurity in public acquisitions require standards that are risk-based and flexible enough to address the continually evolving nature of this global threat, as well as the underlying technology; (2) that policymakers and regulators appropriately balance the essential need to protect critical infrastructure and sensitive data against the Government’s desire to encourage robust competition and participation by both traditional federal contractors and commercial entities; (3) that the existing patchwork of statutes, regulations and policies are harmonized to provide needed consistency and uniformity of approach across the Government; and (4) that the Government make an investment in the training of its acquisition workforce and end users to enable them to recognize the scope of cybersecurity risks and to implement an appropriately risk-based and flexible set of standards.

I. Standards Should Be Risk Based and Flexible

In developing appropriate cybersecurity standards, regulators should (i) establish baseline standards or accreditation for cybersecurity in federal acquisitions that reflect a risk-based approach which acknowledges the diverse array of contractors participating in federal procurements and their need to compete effectively in a global marketplace; (ii) balance the need to incentivize contractors to increase the cybersecurity of their offerings with the risk of creating barriers to entry for participation in federal acquisitions, particularly for smaller companies; and (iii) develop evaluation criteria and contract clauses that appropriately allocate cybersecurity risks and liability in federal acquisitions, while protecting and rewarding companies that proactively incorporate these standards into their products and approaches.

Establishing baseline cybersecurity standards or cybersecurity accreditation requirements as a prerequisite for participation in any federal acquisition carries with it the risks inherent in attempting to standardize security protocols within a rapidly evolving and dynamic sector. A “one size fits all” baseline or accreditation model could lock in a standard based on existing capabilities or threats, rather than allowing the baseline to evolve with technological innovation and adapt to new threats or security risks. Moreover, an acceptable baseline of security controls for critical infrastructure, or for sensitive or highly-sensitive data, would be more demanding than appropriate or necessary for non-critical infrastructure or less sensitive data. In other words, adopting the wrong standard could result in measuring a contractor’s ability to mitigate the wrong kinds of risks. A too-lenient standard could allow participation by firms ill-

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
equipped to address the level of risk expected for the procurement, whereas a too-stringent standard could bar participation of firms otherwise capable of performing the requirement. Neither outcome would serve the best interests of the federal acquisition system.

Given these concerns, any baseline standards or accreditation requirements should be flexible enough to recognize and accommodate different levels of risk, allowing selection of the standard or accreditation calibrated to the cybersecurity risk-level of the procurement. To avoid the “barrier to entry” concern expressed in the RFI, the Government should consider imposing a baseline standard or accreditation appropriate for mitigating the level of cybersecurity risk associated with the procurement. For example, a requirement to implement basic computer protection efforts, such as scanning for malware, viruses, or other threats, may be an appropriate minimal standard for all procurements but is likely insufficient for acquisitions of complex military technology. This tailoring of standards to the risk-level of a procurement would require the Government to engage personnel with appropriate cybersecurity expertise early in the acquisition process, so that the cybersecurity risks could be identified and the appropriate corresponding standards (or relevant sections of standards) or accreditations then detailed in the solicitation.

The Working Group would also benefit from factoring into its deliberations the efforts of several standard-setting organizations that are already engaged in promulgating and updating cybersecurity standards that are widely relied upon by industry. These efforts include the Cybersecurity Framework being developed by the National Institute of Standards and Technology (NIST), the Common Criteria for Information Technology Evaluation (ISO/IEC 15408), and the ISO/IEC 27000-series of information security standards. Given the Government’s preference for commercial solutions and best practices, the Section encourages the Working Group to consider leveraging these existing standards and accreditation models, rather than attempting to “reinvent the wheel” by fashioning government-unique standards or accreditation requirements.

The international nature of the information and communications technology market also augurs against a U.S.-government-unique cybersecurity standard, as such action by the U.S. Government could invite parallel adoption of country-specific cybersecurity requirements by other nations, resulting in a patchwork of potentially conflicting requirements that could stifle innovation and interoperability and potentially frustrate the global competitiveness of U.S. firms. Thus, we believe that the Working Group should attempt to leverage globally accepted standards to the extent feasible.

Finally, to implement a risk-based, flexible approach to maximizing cybersecurity in federal acquisitions successfully, regulators will likely need to develop evaluation criteria and contract clauses that allocate cybersecurity risks and liability appropriately between the acquiring entities, prime contractors, and other entities in the supply chain. As the RFI correctly notes, the “risk owner” is “typically the end user,” which in the case of federal acquisitions is the procuring agency and its employees and support contractors. 78 Fed. Reg. at 27967. Accordingly, we believe that an
appropriate allocation of cybersecurity risks and liability for federal acquisitions is one that “ensure[s] that the risk owner . . . makes the critical decisions about the risk throughout the acquisition lifecycle.” *Id.* The Section recommends that regulators develop cybersecurity evaluation criteria and contract clauses that are consistent with this principle and eschew any temptation to shift liability or risks to prime contractors through evaluation criteria, contract clauses, or other acquisition tools. Furthermore, the acquiring agency and contractors working for it will need to monitor and adapt to continuously evolving cybersecurity risks, which will require ongoing communications and cooperation between and among them, including information sharing and other interactions that could trigger liabilities and risks. The Section recommends that regulators consider and facilitate such ongoing communications in the federal acquisition planning process by developing contract clauses that provide for commercially-based indemnification, waivers, safe harbors, and other liability-related features, where appropriate.

**II. Regulators Should Balance Essential Cybersecurity Needs Against Possible Barriers to Entry**

As noted above, there are inherent tensions between the need to protect critical infrastructure and highly sensitive data, and the desire to permit a wider range of offerors to compete for procurements. A successful approach will depend on the Government implementing flexible and risk-based standards that are adaptable to varied procurements, depending on an assessment of the cybersecurity risks presented by a particular acquisition. For example, to the extent possible, requirements should be technology neutral so as to encourage a greater inclusion of companies and more robust competition.

Commercial companies are essential contributors to the federal marketplace, especially in the electronic technology area. It is in this area, however, where the Government faces some of its most significant vulnerabilities. Thus, commercial companies should be incentivized to incorporate cybersecurity protections throughout their manufacturing and supply chains.

Certain acquisitions involve systems or data so critical or sensitive that an assessment of cybersecurity risks, and identification and imposition of appropriate standards, is essential to ensure that the successful contractor has the capabilities necessary to address potential cybersecurity vulnerabilities. Without appropriate incentives and standards, the Government may remain vulnerable to attack given the prevalence and volume of commercial information technology procured by the Government. At the same time, if security requirements are applied across the board without consideration of the true risks, some of those commercial companies may abandon the federal market, thereby increasing costs for all acquisitions, including those without substantial cybersecurity risk. Such an approach also would increase the Government’s costs, while reducing the level of innovation available through federal acquisitions. Similarly, we suggest that the evaluation criteria for a procurement should be coordinated with the level of cybersecurity risk. For example, in situations where a
procurement presents significant cybersecurity risks, the regulations should generally disfavor a low priced technically acceptable (LTPA) acquisition approach, which would favor the lowest price rather than appropriately managing the cybersecurity needs. If the imposition of cybersecurity requirements is risk based, then the Government will encourage participation from the broadest range of contractors that can meet those requirements. By overstating requirements or by defaulting to a generic set of standards, the Government may discourage both existing contractors and new potential entrants from furnishing the most innovative cybersecurity solutions in the government market.

The Section believes that this approach would allow the Government more flexibility in designing procurements and assigning the appropriate risk-based standards necessary to meet the Government’s cybersecurity goals for a particular procurement.

III. Harmonization of Cybersecurity Requirements and Standards Would Provide Needed Uniformity and Consistency of Approach

The RFI also seeks responses relating to the “harmonization” of cybersecurity requirements and standards at the global, national, state, and local levels. The Section focuses its comments on cybersecurity requirements and standards affecting federal agencies and contractors today. In particular, there are numerous statutes, regulations, and policies addressing a variety of information security standards and requirements. The variations in these statutes, regulations, and polices create significant compliance challenges for contractors doing business with the Government across the spectrum of federal agencies. As a core goal of establishing an information security framework for federal acquisitions, the Government should use this opportunity to provide more consistency and uniformity when applying such requirements and standards. Similarly, to the extent that internal policies and guidance have been developed by federal agencies, those policies and procedures should be published and formalized so as to allow for notice and comment by the contracting community.

A. Federal Cybersecurity Requirements and Standards

Organizations doing business in the public and private sectors face a host of cybersecurity requirements and standards. In the federal sector, such requirements and standards include, among others:

- **FISMA Standards.** The Federal Information Security Management Act (FISMA) governs federal agencies and certain government contractors (44 U.S.C. §§ 3541-49), with more detailed standards provided by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

- **Privacy Act Standards.** The Privacy Act incorporates information security requirements (5 U.S.C. § 552a(e)(9)) applicable to agencies that maintain a “system of
records,” as well as certain contractors involved in the design, development or operation of such records (5 U.S.C. § 552a(m)).

- **HIPAA Standards.** The Health Insurance Portability and Accountability Act (HIPAA), as amended, establishes specific requirements for safeguarding “protected health information” (PHI), with more detailed guidance under the HIPAA Security Rule (see, e.g., 45 C.F.R. § 164.306).


In addition to these federal information security requirements, individual agencies have implemented supplemental requirements in their acquisition regulations and agency-specific policies and directives. See, e.g., Department of Defense Acquisition Regulation Supplement (DFARS) § 239.7102-1; General Services Acquisition Manual (GSAM) § 539.700; Department of Homeland Security (HSAR) § 3004.470; Health and Human Services Acquisition Regulation (HHSAR) Subpart 339.71; National Aeronautics and Space Administration FAR Supplement (NASA FARS) § 1804.470-1.

In addition to these existing requirements, further changes to the FAR and the DFARS have been proposed to address information security and related issues. For example, DFARS Case 2011-D039, Safeguarding Unclassified DoD Information, was proposed to establish standards for safeguarding controlled unclassified information (CUI). 76 Fed. Reg. 38,089 (June 29, 2011). More recently, FAR Case 2011-020, Basic Safeguarding of Contractor Information Systems, was issued to address proper safeguarding of nonpublic government information. 77 Fed. Reg. 51,496 (Aug. 24, 2012).

1. **Variations in Federal Requirements and Standards**

These various statutes, regulations, and policies reflect a variety of information security standards and requirements. As a result of these variations, organizations doing business with the Government face differing rules and standards, resulting in greater challenges and burdens in maintaining compliance across the federal spectrum. Some examples include the following.

- **Notification Periods.** When a security incident occurs, the federal laws and policies impose differing notification periods and standards, ranging from “rapid reporting” (Pub. L. No. 112-239, § 941) to a specified number of
days for such reporting.

- **Notification Content.** As part of the notification requirements, some federal laws specify that the notice include specific details (such as the “technique or method used” in the penetration, a “sample of the malicious software,” and a summary of data compromised), while other laws and policies provide for different content.

- **Data Breach Definition.** The federal laws and policies include differing definitions of data breach, ranging from successful penetration to potentially compromised data.

- **Security Controls.** Some federal laws and directives include detailed security controls (*e.g.*, HIPAA), while others make the choice of security controls subject to risk-based assessments, cost-effective standards, and multi-factor tests (*e.g.*, FISMA).

- **Audit Access.** Regarding the scope of federal government access to private organizations’ networks for assessing the effectiveness of security programs and safeguards, some laws limit federal access to the specific purpose of determining whether agency information was “successfully exfiltrated” and impose duties on the agency to safeguard trade secrets, commercial or financial information, and personally identifiable data (*e.g.*, Pub. L. No. 112-239, § 941); other regulations do not appear to impose such limitations on federal access to a private organization’s information system network and data.

These types of variations in federal information security requirements and standards impose burdens upon organizations whose business spans multiple federal agencies, as each agency may levy requirements that differ in type and scope. In such circumstances, the organizations bear additional compliance burdens and risks of trying to cope with the lack of harmony and consistency in federal cybersecurity requirements and standards.

**2. Internal Agency Guidance**

In addition to these differing information security requirements and standards, many federal agencies incorporate by reference their internal agency directives and instructions into acquisition regulations and individual solicitations. Some examples of such internal guidance being imported into federal acquisitions include the following:

- **DoD Acquisitions.** The DFARS incorporates various
DoD Directives and Instructions by reference into the regulatory clause. *See, e.g.*, DFARS § 239.7102-1.

- **GSA Acquisitions.** The GSAM incorporates by reference such internal guidance as GSA’s CIO IT Security Procedural Guide. *See, e.g.*, GSAM § 539.7001(d).

- **DHS Acquisitions.** The HSAR incorporates by reference its internal policies and directives. *See, e.g.*, HSAR § 3004.470-2.

These agency regulations do not indicate whether these internal directives, instructions, or policies have been published for notice and comment. In general, the Administrative Procedure Act (APA) provides that requirements affecting persons’ substantive rights be published in the Federal Register. 5 U.S.C. § 552(a); *see also NI Indus., Inc. v. United States*, 841 F.2d 1104, 1107 (Fed. Cir. 1988) (declining to enforce internal agency procedures that had not been previously published in the Federal Register). The application and enforcement of the information security requirements and standards should be limited to those that have been published in the Federal Register in accordance with the APA. In addition, the objective of more consistent and uniform federal standards would best be served by relying upon information security requirements that have been subjected to the APA process, particularly the benefit of public review and comment. Such a process has been utilized in promulgating DFARS Case 2011-D039 and FAR Case 2011-020 concerning handling of nonpublic and unclassified information.

**B. State Cybersecurity Requirements and Standards**

Nearly all states have adopted requirements for organizations to provide notification relating to data security breaches. At present, these state requirements lack uniformity:

State laws have helped consumers protect themselves against identity theft while also incentivizing business to have better cybersecurity, thus helping to stem the tide of identity theft. These laws require businesses that have suffered an intrusion to notify consumers if the intruder had access to the consumers’ personal information. The Administration proposal helps businesses by simplifying and standardizing the existing patchwork of 47 state laws that contain these requirements with a clear and unified national requirement.⁴

⁴ *Cybersecurity: Assessing the Nation’s Ability to Address the Growing Cyber Threat: Hearings before the House Comm. on Oversight and Government Reform, 112th Cong. (July 7, 2011) (statement of Greg Schaffer, Acting DHS Undersecretary for National Protection and Programs Directorate)*
Just as variations in federal information security requirements and standards make compliance more difficult and costly, so do such variations in state security breach laws. To lessen this burden on organizations subject to multiple state laws, the goal of consistency and uniformity would be served by greater harmony and consistency through either a “unified” federal standard or a consistent state model law.

IV. Investment in Training and Other Resources for the Acquisition Workforce and End Users is Essential to Applying the Appropriate Standards

The ability of the Government to recognize and differentiate the level of cybersecurity risk inherent in a particular procurement and the standards that should apply to each is crucial to successful implementation of flexible, risk-based cybersecurity requirements.

A foundational element to the feasibility of cybersecurity standards in the federal acquisition system is a common set of definitions. As addressed elsewhere in these comments, federal contractors are already subject to a range of cybersecurity standards spanning international, federal, and state regimes (in addition to separate commercial standards). Cyber and information security in the federal space is further segmented into agency-specific standards. These differing regimes often apply distinct definitions to terms that are key to the applicability of security standards; these definitions may not always be consistent across regimes. In light of this issue, DoD and GSA should consider the feasibility of adopting common definitions in the security standards developed for federal acquisitions. A common set of definitions that spans all agencies (and, perhaps, state and local agencies leveraging federal standards) would likely make any new standard more feasible, which in turn would help contractors more effectively apply cyber and information security protections.

Another key factor in making new cybersecurity standards feasible will be the ability of the federal acquisition workforce to understand these standards and apply them consistently with the level of risk applicable to any particular requirement. Acquisition professionals engage in significant acquisition planning activities long before contractors become involved in the acquisition process. These professionals therefore have significant responsibility for understanding the cybersecurity risk inherent in an acquisition, and applying standards appropriate to address the risk. Acquisition professionals will also need to be cognizant of cybersecurity standards when addressing issues during the course of contract performance. These standards may come into play in the event of a cyber attack or similar type of emergency; they may be common to traditional performance matters such as requests for equitable adjustment and claims for costs. Adequate training in cybersecurity standards and requirements will assist acquisition professionals to better apply those standards throughout the course of the acquisition lifecycle. Moreover, mechanisms need to be assessed and implemented so as to provide necessary and appropriate levels of expert evaluation and guidance regarding these cybersecurity considerations at every relevant

stage of the acquisition process, from procurement planning through contract administration.

Finally, programs that include funding for end-user education would also provide valuable assistance in improving cybersecurity. Educating the end customer on important steps that should be taken, from the use of adequate passwords to the encryption of data, would help to reduce the security risks in systems that are subject to cyber attack.

V. Conclusion

The Section appreciates the opportunity to provide these comments on the RFI. We are available to provide additional information or assistance as you 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
Chairs, Cybersecurity, Privacy and Data Protection Committee
Kara M. Sacilotto
Craig M. Smith
Judith Miller, Co-Chair, ABA Cybersecurity Legal Task Force
Harvey Rishikof, Co-Chair, ABA Cybersecurity Legal Task Force