September 10, 2015

Via Online Portal

The Office of Management and Budget
725 17th Street NW
Washington, DC 20503


Dear Sir or Madam:

On behalf of the Section of Public Contract Law (“Section”) of the American Bar Association (“ABA”), I am submitting comments on the Office of Management and Budget’s (“OMB”) draft guidance titled “Improving Cybersecurity Protections in Federal Acquisitions” (issued August 11, 2015).1 The ABA consists of attorneys and associated professionals in private practice, industry, and government service. The ABA and its Sections’ governing Councils 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.2 The views expressed herein 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 policy of the ABA.3

The draft guidance makes several important contributions toward achieving its objective, including distinguishing the requirements that should apply to systems operated “on behalf of the Government” from those that should apply to contractor internal systems that include controlled unclassified information (“CUI”). In addition, the draft guidance takes some positive initial steps for much needed harmonization that will facilitate the ability of all contractors, including small businesses, to improve their and our nation’s cybersecurity. Nonetheless, the Section believes that certain aspects of

1 OMB has posted the draft guidance at https://policy.cio.gov.

2 Mary Ellen Coster Williams, Section Delegate to the ABA House of Delegates, and Heather K. Weiner and Anthony N. Palladino, 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.

3 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.”
the draft guidance should be revised or reconsidered before its issuance. The Section believes these proposed revisions or considerations will not diminish the objective of strengthening cybersecurity protections, but instead will result in improved compliance with strengthened cyber protections that will benefit the Government and the contracting community alike.

Because OMB has requested comments be made through discussions on a publicly-accessible portal hosted at https://github.com/WhiteHouse/cyber-acquisitions/issues, the Section has created five separate “issues” (i.e., comment threads) on the portal, each with comments specific to one of the five topics addressed in the draft guidance. The issues (threads) are titled as follows:

- Comments on Security Controls (ABA Public Contract Law Section [“PCLS”]);
- Comments on Information Security Continuous Monitoring (ABA PCLS);
- Comments on Cyber Incident Reporting (ABA PCLS);
- Comments on Information System Security Assessments (ABA PCLS); and
- Comments on Business Due Diligence (ABA PCLS).

The Section notes in this regard that breaking up comments into these various topics and submitting them through different electronic portal threads may dilute the ability of the Administration and public to understand the nature and extent of comments and concerns relating to the proposed guidance. In addition, this approach may make accessing responsive comments more difficult and time-consuming, and thus make the drafting and revision process less transparent. The Section suggests that OMB establish a formal location for the preservation of and public access to the guidance and responsive comments, such as at regulations.gov.

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

Sincerely,

David G. Ehrhart
Chair, Section of Public Contract Law

cc:
James A. Hughes
Aaron P. Silberman
Kara M. Sacilotto
Council Members, Section of Public Contract Law
Chairs and Vice Chairs, Cybersecurity, Privacy, and Data Protection Committee
Craig Smith
Samantha S. Lee
American Bar Association Section of Public Contract Law
Comments on OMB’s Draft Guidance
“Improving Cybersecurity Protections in Federal Acquisitions”

Security Controls

The Section of Public Contract Law (“Section”) of the American Bar Association concurs that it would serve the interests of both the Government and industry to address enhanced cybersecurity controls for systems operated on behalf of the Government and for internal contractor systems that include controlled unclassified information (“CUI”), in light of the evolving cyber threat environment. The Section agrees with the draft guidance’s recognition that different baseline security standards should apply to systems operated on behalf of the Government versus contractor internal systems with CUI (i.e., National Institute of Standards and Technology (“NIST”) Special Publication (“SP”) 800-53 versus NIST SP 800-171). The draft guidance specifically acknowledges that “the application of NIST SP 800-53 controls [to contractors’ internal systems that incidentally contain CUI] is generally not appropriate.”

The draft guidance recognizes the security of information systems should be “clearly, effectively, and consistently addressed in Federal contracts.” Consistent with that understanding, the Section recommends that the security controls applicable to contractor internal systems that include CUI be uniformly applied across the Government. Such harmonization is consistent with the Cybersecurity Executive Order that required acquisition regulators to “address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.” Such harmonization would also serve other fundamental principles governing federal acquisitions and cybersecurity needs, including regulatory consistency, cost-effective cybersecurity, greater competition, and enhanced cybersecurity:

- **Regulatory Uniformity.** As its core purpose, the Federal Acquisition Regulation (“FAR”) seeks “uniform policies and procedures for acquisition by all executive agencies.” FAR 1.101; see also FAR 1.302.

- **Cost Effective Cybersecurity.** As a key principle, federal law requires that agencies’ cybersecurity programs and risk analyses consider cost-effectiveness (see, e.g., 44 U.S.C. § 3554), a factor likely to be enhanced by uniform acquisition regulations governing cybersecurity.

- **Greater Competition.** Like the Federal Risk and Authorization Management Program (“FedRAMP”) objective for federal cloud cybersecurity (“approve once, use often”), uniform acquisition regulations for cybersecurity would encourage competition by reducing the burden for contractors—particularly small businesses—to comply with cybersecurity requirements. See, e.g., 10 U.S.C. § 2304(a)(1)(A) (specifying “full and open competition”).

---

1. See https://policy.cio.gov.
2. See id.
**Enhanced Cybersecurity.** In response to the Cybersecurity Executive Order, both the Department of Defense and the General Services Administration acknowledged that harmonized acquisition regulations would enhance cybersecurity.4

Such harmonization of security controls, wherever possible, is crucial to enhancing our cybersecurity posture in light of the technical complexities and significant costs of implementing such safeguards and the scarcity of skilled cybersecurity resources to implement those solutions. As noted in NIST SP 800-171, a forthcoming single FAR clause “will further promote standardization to benefit a substantial number of nonfederal organizations that are attempting to meet the current range and type of contract clauses, where differing requirements and conflicting guidance from federal agencies for the same information gives rise to confusion and inefficiencies.”5

The Section recognizes that under certain circumstances individual agencies may need to tailor the recommended security controls to account for unique risks or legal or governmentwide policy requirements associated with a particular system operated on behalf of the Government. The Section recommends, however, that OMB encourage as much harmonization as possible. Variations in federal information security requirements and standards make compliance more difficult and costly, and could undermine the goal of enhancing cyber protections.

In that spirit, the Section also recommends that OMB consider revising the draft guidance to adopt language similar to a clause at Defense Federal Acquisition Regulation Supplement (“DFARS”) 252.204-7012, “Safeguarding Unclassified Controlled Technical Information,” which had been effective until a DFARS interim rule published on August 26, 2015.6 DFARS 252.204-7012 permitted contractors to deviate and/or propose alternatives to specified security controls. In particular, the clause had allowed contractors the flexibility of suggesting an alternative to a required control by submitting a written explanation to the contracting officer of one of the following:

(A) How the security control identified by the then-existing DFARS rule did not apply; or

(B) How an alternative control or protective measure could be used to achieve equivalent protection.7

The inclusion of such flexibility would enable companies to take advantage of the cybersecurity efforts that have already been undertaken (and the associated sunk costs) by

---

5 NIST SP 800-171, at iv.
6 On August 26, 2015, DoD published an interim rule removing the existing DFARS 252.204-7012 and replacing it with a new clause, Safeguarding Covered Defense Information and Cyber Incident Reporting. See Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018). 80 Fed. Reg. 51739 (Aug. 26, 2015). This interim rule was recently issued and comments on that rule are due by October 26, 2015.
many contractors to comply with industry standards or with requirements that have been imposed by individual government agencies.

In addition, such flexibility is critical to the objectives of the Federal Acquisition Streamlining Act ("FASA") and FAR part 12 that promote the acquisition of commercial items. In FASA’s legislative history, Congress recognized that restrictive acquisition provisions had limited federal agencies’ access to technologies widely available in the commercial marketplace.8 As the first step in remedying this problem, Congress directed federal agencies to acquire commercial items “to the maximum extent practicable.”9 Thus, when applied to the acquisition of commercial items, the federal security requirements should include flexibility for revision to be consistent with commercial practices to the maximum extent practicable.10

Finally, the draft guidance does not address certain key implementation issues that should be considered before the security controls section is finalized. For example, the draft guidance does not specifically address what information constitutes CUI. The Section notes that the long-standing National Archives and Records Administration (“NARA”) effort under Executive Order 1355611 has still not advanced past a proposed rule.12 Consistent with the prior version of DFARS 252.204-7012, we recommend that the draft guidance require government marking of data to trigger classification and protection as CUI.13 Contractors need these markings to identify the data subject to government controls to be housed in a compliant section of their networks. The draft guidance also does not address when contractor internal systems will need to be compliant with NIST SP 800-171, which was just issued as final guidance to federal agencies in June 2015 and is a robust document with many requirements and provisions. For small and mid-size companies with less mature cybersecurity measures in place, compliance will not be achieved without a significant expenditure of costs, time, and resources, with much required from external sources. Lastly, we recommend that the final guidance clarify that legal authority to require compliance with reporting obligations presently allows for imposing these requirements only on a contractual basis—either on (a) a prime contractor that has received or produced CUI under a government contract, or (b) a subcontractor that has received CUI from a higher-tier contractor or has produced such CUI while performing a government subcontract.

The Section’s complete comments on OMB’s draft guidance are available in a consolidated pdf at http://www.americanbar.org/groups/public_contract_law/

9 FASA, Pub. L. No. 103-355, § 8104(b), as reprinted in 1994 U.S.C.C.A.N. 3243, 3391; see also 10 U.S.C. § 2377(b); FAR 1.102(b)(1)(i) (“Maximizing the use of commercial products and services”), FAR 1.102-2(a)(4) (same), FAR 12.101 (“Acquire commercial items . . . when they are available”).
10 FASA, Pub. L. No. 103-355, § 8002 reprinted at 1994 U.S.C.C.A.N 3386 (to maximum extent practicable, agencies must only use contract clauses in commercial item acquisitions that “are determined to be consistent with standard commercial practice”); see also FAR 12.301(a) (same).
resources/prior_section_comments.html under the topic “Cybersecurity; Access to and Protection of Information.”

* * * * *
The Section of Public Contract Law (“Section”) of the American Bar Association understands that continuous monitoring is increasingly important in assuring controlled unclassified information (“CUI”) and other controlled information remains secure. The Section also recognizes that Information Security Continuous Monitoring (“ISCM”) will be a key consideration in assuring adequate cybersecurity protections in federal acquisitions. The Section, however, has identified two sections of the guidance that would benefit from greater clarity around the factors that agencies should consider in setting the standards for ISCM.

First, although the draft guidance contemplates that agencies may need the assistance of the Department of Homeland Security’s (“DHS”) Continuous Diagnostics and Mitigation (“CDM”) program to “establish[] ISCM capabilities quickly,” the draft guidance also recognizes that it may not always be “feasible” to provide this tool to contractors operating information systems on behalf of the Government. Even if DHS’s CDM is not provided, the contractor-operated system must still meet or exceed the information security continuous monitoring requirements identified in OMB Memorandum M-14-031; and the agency may elect to perform information security continuous monitoring and IT security scanning of contractor systems with tools and infrastructure of its choosing.

The cost in terms of time and resources necessary to create a system satisfying the requirements of M-14-03 could operate as a barrier to entry, particularly for small and mid-size businesses, which often lack the advantages of strategic sourcing to implement ISCM protections in their systems and have fewer resources available to develop ISCM capabilities. This barrier to entry is all the more disconcerting if agencies will have unfettered discretion to determine that it is “not feasible” to provide DHS’s CDM capabilities to a contractor operating information systems on behalf of the Government. Without knowing what factors an agency may consider in determining the feasibility of providing DHS’s CDM capabilities to contractors, it is difficult for contractors to undertake the business planning and resource allocation necessary to be ready to implement ISCM protections and “work together [with agencies] to determine and implement an appropriate solution that fulfills the ISCM requirements.” Thus, the Section encourages OMB to require agencies to consider the capabilities and availability of small business and mid-size contractors when determining the feasibility of providing DHS’s CDM capabilities to contractors operating information systems on their behalf.

Another potential barrier to entry is the discretion that the draft guidance would grant to agencies to “perform information security continuous monitoring and IT security scanning of contractor systems with tools and infrastructure of its choosing.” The Section

---

1 This memorandum is available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.
recommends that the draft guidance require agencies to communicate with the contracting community (and particularly small and mid-size businesses) and information-security standard-setting organizations regarding the factors it will consider in determining the tools and infrastructure it will use for ISCM monitoring. Further, the Section urges agencies to seek consistency in the tools and infrastructure used for monitoring. This consistency will enable the contracting community to better prepare to satisfy agencies’ ISCM needs and increase the number of contractors available to the Government.

The Section’s complete comments on OMB’s draft guidance are available in a consolidated pdf at http://www.americanbar.org/groups/public_contract_law/resources/prior_section_comments.html under the topic “Cybersecurity; Access to and Protection of Information.”

* * * * *
American Bar Association Section of Public Contract Law  
Comments on OMB’s Draft Guidance  
“Improving Cybersecurity Protections in Federal Acquisitions”  
Cyber Incident Reporting

The Section of Public Contract Law (“Section”) of the American Bar Association understands the need for and supports the draft guidance’s requirement that contractors provide reports to the Government of cyber incidents on systems being operated on behalf of the Government and, to the extent controlled unclassified information (“CUI”) is affected, cyber incidents on contractors’ internal systems. The limitation of the reporting obligations for internal systems to those incidents affecting CUI is consistent with the preexisting DFARS clause.¹ The Section believes, however, the draft guidance could be clarified in a number of areas.

The draft guidance does not define CUI or identify the marking requirements for CUI.² For contractors to protect CUI appropriately in accordance with National Institute of Standards and Technology Special Publication 800-171 and to ascertain effectively whether a cyber incident affects CUI within mandatory reporting timeframes, it is essential for the Government to identify and mark covered information as CUI. The Government needs not only to mark any CUI before it is shared with contractors, but also to provide clear direction to contractors who will generate information containing CUI. The Section encourages the Office of Management and Budget to clarify in the draft guidance that the reporting obligation applies only when appropriately marked CUI is affected.

The draft guidance also does not specifically address subcontractor reporting. The Section recommends that subcontractors be given the flexibility to report cyber incidents directly to the Government rather than through their prime contractors or higher-tiered subcontractors. Permitting this streamlined reporting function will avoid unnecessary delays in reporting up through contracting levels, and mitigate potential concerns about disclosure of proprietary information to prime and higher-tier contractors.

The Section recognizes that although tailored reporting requirements may be necessary to reflect varying priorities of particular agencies, agencies should nonetheless be strongly encouraged to comply with a common, streamlined reporting process to the extent practicable so that valuable time is not focused on ascertaining applicable requirements rather than mitigating any potential threat. Candidates for standard processes include timelines for reporting breaches, contents of reports, and designations of where to file reports. In particular, the draft guidance appears to require notices to multiple officials on every contract affected, which may provide little or no value while generating cost and reporting delays. The Section would encourage, to the extent available and feasible, that the agencies leverage existing centralized reporting mechanisms such as the Defense Industrial Base reporting system to minimize the costs

¹ See DFARS 252.204-7012(d)(1).
² A pending rule from the National Archives and Records Administration (“NARA”), discussed in our separately posted comments on security controls, does identify a process for identifying and marking CUI.
and confusion associated with duplicative reporting. The Section believes that centralized reporting would promote coordinated response activities, whereas reporting to every potentially interested government official will delay and disperse the efforts to investigate, mitigate, and correct cyber incidents.

The Section would also encourage the final guidance to recognize that reporting should be an iterative process. The initial report should notify the Government of the cyber incident with follow-up as necessary to address the results of an assessment of the scope of the incident, mitigation of the disclosure, and corrective action to prevent reoccurrence.

Finally, the Section notes that some categories of CUI (e.g., information subject to the International Traffic in Arms Regulations (“ITAR”)) may not as a matter of law be governed or managed by the customer agency itself. Consequently, we recommend that the final guidance specify that any assessment of the consequences of a disclosure of such categories of CUI should remain the province of the agency responsible by law for the information (in the case of the ITAR, the State Department) and should be an independent matter for the contractor to assess and report upon as appropriate to that agency. In addition, mandatory cyber incident reporting should not obviate any protections afforded by such regulating agency’s voluntary disclosure programs.

The Section’s complete comments on OMB’s draft guidance are available in a consolidated pdf at http://www.americanbar.org/groups/public_contract_law/resources/prior_section_comments.html under the topic “Cybersecurity; Access to and Protection of Information.”

* * * * *
American Bar Association Section of Public Contract Law
Comments on OMB’s Draft Guidance
“Improving Cybersecurity Protections in Federal Acquisitions”
Information System Security Assessments

The draft guidance requires agencies to develop an approach to assessing the security of information systems operated by contractors, including an assessment by the senior agency official for privacy as to the level of necessary privacy controls. The Section of Public Contract Law (“Section”) of the American Bar Association agrees with the recognition in the draft guidance that differing approaches may be appropriate depending on the information systems and data at issue. It would be helpful, however, if the Office of Management and Budget (“OMB”) revised the draft guidance to specify which portions of the guidance on information system security assessments apply to information systems managed “on behalf of” the Government and which portions apply to internal contractor systems that contain controlled unclassified information (“CUI”).

The Section applauds the draft guidance’s recognition that many contractors operating in the commercial market already receive a variety of independent assessments that may be useful for assessing the security of contractor systems. Consistent with the Federal Acquisition Streamlining Act and the Federal Acquisition Regulation’s promotion of commercial item contracting, OMB should maintain this flexibility as the guidance is finalized. Further clarification as to which independent assessments would meet the Government’s needs would allow contractors to allocate resources in a meaningful way and to plan appropriately.

There are two areas of the draft guidance where the Section notes concerns. First, in the assessment process, contractors will be required to give agencies access to the contractors’ “facilities, installations, operations, documentation, databases, IT systems, devices, and personnel used in performance of the contract, regardless of location.”1 The draft guidance does not limit this access. This unlimited access would be a concern because contractor information is commingled with trade-secret, proprietary, privileged, and/or third party data subject to non-disclosure requirements. The Section recommends that the final guidance recognize these limitations. For example, a clause at Defense Federal Acquisition Regulation Supplement (“DFARS”) 252.204-7012, “Safeguarding Unclassified Controlled Technical Information,” which was effective until a DFARS interim rule published on August 26, 2015, provided that the obligation to share data in a post-cyber incident assessment “exists unless there are legal restrictions that limit a company’s ability to share digital media.”2 The Section recommends that OMB include a similar recognition in the final guidance regarding any potential government access to contractor systems.

Second, the draft guidance states that agencies will be required to specify in each solicitation how contractors will be required to demonstrate that they meet the requirements of National Institute of Standards and Technology Special Publication 800-

---

1 See https://policy.cio.gov.
2 DFARS 252.204-7012(d)(5) (Nov. 2013 version replaced by interim rule on August 26, 2015).
171, including a security assessment for contractor internal systems. The draft guidance indicates that could require submissions ranging from a simple attestation of compliance to a “detailed description of the system’s security architecture, controls and provision of supporting test data."\(^3\) The Section recommends that any requirement to share this extremely sensitive data in proposals be eliminated from the guidance given the security concerns contractors will have with providing the Government (or any third party) with detailed information in writing about their security architecture or controls. These concerns will be amplified when this information would have to be shared with the Government electronically because such government portals and websites are often targeted for access by unauthorized groups and individuals.

The Section’s complete comments on OMB’s draft guidance are available in a consolidated pdf at http://www.americanbar.org/groups/public_contract_law/resources/prior_section_comments.html under the topic “Cybersecurity; Access to and Protection of Information.”

* * * * *

\(^3\) See https://policy.cio.gov.
The draft guidance to agencies would modify current pre-award and post-award business due-diligence processes to add a cybersecurity element. The draft guidance suggests leveraging a current General Services Administration (“GSA”) pilot to create a business due-diligence information shared service, which would provide agencies with access to various types of “risk information,” with data collected from multiple sources, including public records, publicly-available and commercial-subscription information, and voluntary contractor reporting. The Section of Public Contract Law (“Section”) of the American Bar Association identifies below areas that the Section believes require further attention and detail from the Office of Management and Budget (“OMB”).

First, the Section believes that this part of the draft guidance does not clearly state whether this new requirement would apply only to acquisitions and contracts in which systems are being operated on behalf of the Government or whether it also would extend to any procurement that would involve contractor access to controlled unclassified information.

The Section recommends that the OMB carefully consider any potential detrimental use of voluntary reporting of incidents by contractors. Information sharing is a critical component of effective cybersecurity and we suggest that the Government should refrain from using voluntary disclosures against participants. The Section further notes that the use of such data for acquisition purposes may violate the fundamental confidentiality obligations and use limitations agreed to by the Government in industry information-sharing framework agreements1 and in some of the proposed information sharing legislation now being considered in Congress.2 Indeed, the use of prior incidents as a negative in business due-diligence assessments could harm those companies that already have robust information security systems, with features including continuous monitoring and other mature cyber defenses in place, which would have made them more cognizant of and able to report on such matters even before the issuance of this policy.

Although the draft guidance refers to the collection and utilization of such data as based “on transparent, objective, and measurable risk indicators,”3 the draft guidance does not define what those indicators will be. Rather, OMB contemplates that, within 90 days of publishing the final guidance, an interagency cyber team will work with GSA to develop and recommend the specific risk indicators that should underlie this cyber due-

---

1 See DFARS part 236, Department of Defense (DOD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities; see also http://dibnet.dod.mil/staticweb/Register.html


3 See https://policy.cio.gov.
diligence process. The Section recommends that the working group allow industry comment on any indicators before they are finalized.

The draft guidance also does not address how cyber due diligence will be used by the Government and whether contractors will be permitted input into any assessments that the Government makes based on this information.

Ultimately, unlike for the other four sections in the draft guidance, here OMB does not contemplate that this effort will be part of a forthcoming Federal Acquisition Regulation rulemaking. The draft guidance raises significant questions, including potential legal issues relating to de facto debarment and rulemaking requirements. In light of the relatively less mature status of this part of the draft guidance compared with the other recommendations, we recommend that the business due-diligence section be deleted from the guidance and be distributed separately in draft form for public comment and that any rule on this be issued in accordance with procurement rulemaking requirements once the matter is more clearly defined so that a similar level of transparency can be achieved with this important issue.

The Section’s complete comments on OMB’s draft guidance are available in a consolidated pdf at http://www.americanbar.org/groups/public_contract_law/resources/prior_section_comments.html under the topic “Cybersecurity; Access to and Protection of Information.”

* * * * *

---

4 A process that would result in debarment of a government contractor requires affording the contractor due process. See, e.g., FAR subpart 9.4. Procurement rules in general require rulemaking notice and comment as well. See, e.g., 41 U.S.C. § 1707(a).