November 20, 2015

Dear Mr. Pitsch:

On behalf of the American Bar Association (“ABA”) Section of Public Contract Law (“Section”), I am submitting comments on the interim rule cited above.1 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 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.2

1 Mary Ellen Coster Williams, Section Delegate to the ABA House of Delegates, and Heather Weiner, 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.

2 This letter is available in pdf format at http://www.americanbar.org/groups/public_contract_law/resources/prior_section_comments.html under the topic “Cybersecurity; Access to and Protection of Information.”
I. INTRODUCTION

The Section recognizes the critical importance of implementing enhanced cybersecurity protections and sound cloud-acquisition rules, particularly in light of the evolving cybersecurity threats to the Government and its contractors. The Department of Defense (“DoD”) and the Defense Industrial Base (“DIB”) have a strong record of working collaboratively to address these cyber issues and this close cooperation in the past has led to successful cyber initiatives, including the piloting of the DoD’s voluntary information-sharing program, which ultimately was implemented into regulation.3

The Section is concerned about DoD’s decision to issue an interim rule rather than a proposed rule given the state of rulemaking in this area. The Section notes in this regard that the long-standing National Archives and Records Administration (“NARA”) effort under Executive Order 13556, Controlled Unclassified Information,4 still has not advanced beyond a proposed rule5 and a final government-wide Federal Acquisition Regulation (“FAR”) clause is not expected until at least 2016.6 In light of this timing, issuing a proposed rule would provide a much needed opportunity for affected companies to assess the new rules fully and provide substantive input before the rule takes effect. As discussed in more detail below, the interim rule mandates compliance with new cyber rules that by their very nature require significant time and resources to implement and that raise significant legal and compliance issues. As always, the Section appreciates the opportunity to comment on the interim rule.

II. COMMENTS

The Section recommends that DoD revise the interim rule in the following areas.

A. The Rule Lacks Certainty About what Will Be Deemed Covered Defense Information Subject to Safeguarding Requirements.

1. The Interim Rule Should Require DoD to Identify and Mark Covered Information.

The interim rule’s definitions do not provide contractors and subcontractors adequate notice regarding what information is subject to the enhanced safeguarding and reporting requirements. In response to public comments expressing concerns about conflicting policies, lack of clarity in categories and markings, and difficulty in distinguishing between the need for basic and enhanced safeguarding, DoD limited the scope of the prior Defense Federal Acquisition Regulation Supplement (“DFARS”) rule

---

3 See DFARS Part 236.
6 National Institute of Standards and Technology Standard Procedure 800-171, at vi.
regarding safeguarding of information in its final version. DoD limited the prior DFARS rule to limit the application of safeguarding controls only to unclassified controlled technical information (“UCTI”) marked in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents (“prior UCTI rule”). Requiring that DoD mark information subject to safeguarding requirements under the prior UCTI rule provided fair notice and served as a crucial and appropriate limitation on contractor and subcontractor liability. In contrast to the prior UCTI rule and the explicit expectation in the proposed NARA Rule on Controlled Unclassified Information, the interim rule does not obligate DoD to mark all covered defense information as such.

In addition to concerns about fair notice, there are practical reasons not to shift the onus to contractors to make decisions about categorizing information. For several reasons, the Government bears an inherent responsibility to determine which of its information should be safeguarded as sensitive and which should be available to the public. First, a broad range of statutes and policies impose transparency obligations on federal agencies and operations. Second, the Government must perform its own risk assessments, define its own security objectives, and identify the risks to national security or other interests that would bear upon decisions about which information must be secured. Third, the National Institute of Standards and Technology (“NIST”) Special Publication (“SP”) 800-171 cited in the interim rule encourages the use of information-system architectures that allow for segregation of data so that enhanced safeguarding need be applied to only part of a contractor’s information architecture. If, however, contractors will be expected to safeguard unmarked information, the task of identifying and segregating such information for safeguarding will be materially more difficult and costly, bordering on impossible. Even worse, lower-tier and commercial subcontractors who may not deal directly with DoD will need to recognize and safeguard categories of unmarked information, often with limited experience and resources to do so.

The Section recommends that DoD revise the interim rule, consistent with the prior UCTI rule, to limit its application only to covered defense information marked as protected by DoD.

---

8 This requirement for government marking was acknowledged in Frequently Asked Questions issued by DoD with regard to the prior DFARS rule. See http://www.acq.osd.mil/dpap/pdi/docs/ControlledTechnicalInformation_FAQ.pdf.
9 See 80 Fed. Reg. at 26508 (§ 2002.15(a)(7)).
2. All Four Categories of CUI Would Benefit from Further Clarification.

Under the interim rule, covered defense information is controlled unclassified information ("CUI") within one of four defined categories that is either (1) provided to the contractor in connection with a DoD contract, or (2) collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of contract performance. The definitions of each of these four categories would benefit from further clarification.

a. Controlled Technical Information

Controlled technical information is defined as follows:

[T]echnical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.\[^{12}\]

Although the definition of controlled technical information above is similar to the definition of UCTI under the prior UCTI rule, there is one important distinction. Rather than limiting the definition of controlled technical information to marked data, the new definition includes any information that would meet the criteria for marking in DoD Instruction 5230.24, regardless of whether the information is marked. The Section has three concerns. First, DoD Instruction 5230.24, which is not subject to notice-and-comment rulemaking, would be given regulatory effect by this definition. Second, that instruction includes no meaningful guidance for a contractor to follow when determining what constitutes controlled technical information. Finally, the instruction itself characterizes the assigning of a specific distribution statement as an “inherently Governmental responsibility.”\[^{13}\] Additionally, the rule provides that information “lawfully publicly available without restriction is not covered.”\[^{14}\] This is such a vague carve out as to render compliance with the interim rule impossible. How is a contractor or subcontractor to know whether information is not lawfully available without restriction if, for example, it finds that it is posted on a commercial website?

\[^{11}\] DFARS 204.7301.
\[^{12}\] Id.
\[^{13}\] DoD Instruction 5230.24 at 9, § 7(b).
\[^{14}\] DFARS 204.7301.
To clarify contractors’ obligations, the Section suggests retaining the prior UCTI rule’s definition, under which controlled technical information must be safeguarded only if it is marked by the Government in accordance with DoD Instruction 5230.24. If, and to the extent, DoD expects a contractor or subcontractor to safeguard information that it creates, DoD could adopt the guidance it provided with the prior UCTI rule directing contracting officers to provide specific and clear instructions for identifying and marking controlled technical information that is expected to be produced under the contract. This approach would allow for clarity and ensure that contracts with unique requirements are appropriately addressed and that information to be controlled is clearly and easily identifiable.

b. Critical Information (Operations Security)

Critical information (operations security) is defined as follows:

Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).[16]

Under this definition, critical information is limited to “[s]pecific facts identified through the Operations Security process.”[17] DoD’s relevant Operations Security (“OPSEC”) Program Manual, 5205.02-M, states in Enclosure 6: “Requirements for OPSEC must be included in the contract solicitation and resulting contract in sufficient detail to ensure complete contractor understanding of all OPSEC provisions required.” The DFARS clause and the cited manual presuppose that DoD will have completed an OPSEC analysis, clearly communicated the OPSEC provisions to be applied, and identified the specific facts to be protected.

If that OPSEC process is not completed, and critical information is not included in the contract solicitation in sufficient detail to ensure complete contractor understanding, contractors and subcontractors will not be able to safeguard critical information. By its nature, designating critical information depends upon discretion and subjective assessments of risks that will often require information uniquely within the Government’s control. The Section recommends clarifying the definition to include the following statement from the relevant OPSEC Program Manual: “Requirements for OPSEC must be included in the contract solicitation and resulting contract in sufficient detail to ensure complete contractor understanding.”

[16] DFARS 204.7301.
[17] Id. (emphasis added).
c. Export Control

Export control is defined as follows:

Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.[18]

In some respects, adding export control as a category of information to be protected builds upon the prior UCTI rule, because much of UCTI under that rule was co-extensive with International Traffic in Arms Regulations ("ITAR") controlled technical data. The reference to export controls is a helpful clarification, however, because the prior UCTI rule was not explicit about it likely covering a portion of government-generated information or technical data marked as subject to the ITAR.

The scope of the interim rule’s reference to export controlled information, nonetheless, could be further clarified. Substantial portions of non-publicly-available U.S.-origin technical information are potentially subject to U.S. export controls under the Export Administration Regulations ("EAR"). Much of the information so controlled falls under the catch-all low-level category of EAR 99. For instance, a drawing describing how to produce a tennis ball may technically be subject to the EAR. The interim rule is not likely intended to be so broad as to encompass all U.S.-origin technical information. Instead, the interim rule is likely intended to protect only information and technical data controlled under the ITAR or EAR for reasons of national security and nonproliferation. This is a logical conclusion given the interim rule’s reference to the compromise of national security and nonproliferation objectives, which are not defined in the ITAR but are specific categories of control on the Commerce Control List of the EAR covering a much narrower range of items and information.

The Section encourages DoD to revise the definition of export control to specify which types of export-controlled information are subject to the interim rule’s safeguarding requirements. Broadly construed, the interim rule could conceivably cover vast swathes of low-level, non-critical export-controlled information. The Section encourages DoD to define “export controlled information” as particular categories of ITAR-controlled technical data, as well as technical data controlled under designated control-list categories of the EAR, such as national security, nonproliferation, and missile technology.

[18] Id.
d. Any Other Information, Marked or Otherwise Identified in the Contract

The interim rule contains a catch-all provision that provides as follows:

Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).19

Catch-all provisions are often problematic, threatening to regulate further than is necessary, beneficial, or intended. Such provisions pose particular concerns in the context of information security given the broad statutory obligations imposed upon federal agencies to assure transparency and openness in Government.

The provision of the definition that includes “or otherwise identified in the contract” is very broad and could create confusion as to what falls within this requirement. The Section appreciates that it may also be necessary or useful in some situations to provide instruction as to how to identify rather than mark information, such as information that will be created by the contractor during performance. The Section believes, however, that further clarification is necessary to ensure that the final rule is consistent with the Government’s transparency obligations and its security framework for the safeguarding of CUI. Specifically, the catch-all provision should be revised to make clear that safeguarding obligations are limited to those specific categories and subcategories of CUI included within the CUI registry.

B. Changing the Security Controls, Effective Immediately, Does Not Recognize the Realities of Information Security and Does Not Support the Goal of Harmonization.


Both the prior UCTI rule and interim rule require contractors to provide “adequate security.”20 The definition of “adequate security” is identical in both rules: “protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.”21 One of the interim rule’s most fundamental changes, however, is the switch in the security-control standard that sets the minimum baseline for “adequate security” for companies’ covered contractor

19 Id.
20 See DFARS 252.204-7012(b) (Aug. 2015); DFARS 252.204-7012(b) (Nov. 2013).
21 See DFARS 252.204-7012(a) (Aug. 2015); DFARS 252.204-7012(a) (Nov. 2013).
information systems, \textit{i.e.}, internal contractor systems that process, store, or transmit covered defense information.\textsuperscript{22}

The prior UCTI rule, which focused solely on protecting marked UCTI, required covered contractor information systems to meet, at a minimum, certain specified security controls in NIST SP 800-53 to comply with the adequate-security requirement.\textsuperscript{23} In publishing the final version of the prior UCTI rule, DoD suggested that the selected controls from NIST SP 800-53 “closely parallel the ISO 27002 standard” and “[a]s such, the controls represent mainstream industry practices.”\textsuperscript{24} DoD further indicated that “[w]hile there is a cost associated with implementing information assurance controls, the use of industry practices provides assurance the costs are reasonable.”\textsuperscript{25}

The interim rule, however, requires contractor systems to comply with all NIST SP 800-171 security controls, or, as discussed in Section C below, equally-effective alternative controls approved by the DoD Chief Information Officer (“CIO”). NIST SP 800-171 was published in late June of this year\textsuperscript{26} in anticipation of the finalization of the federal CUI regulation.\textsuperscript{27} Unlike NIST SP 800-53, which was developed to identify Federal Information Security Management Act (“FISMA”)-compliant information security controls for federal information systems, NIST SP 800-171 was specifically developed to define security requirements for protecting CUI in nonfederal information systems.\textsuperscript{28}

As set forth in more detail in Section B.4 below, the requirements imposed by NIST SP 800-53 and NIST SP 800-171 are very different. The interim rule’s imposition of the new NIST SP 800-171 requirements, effective immediately, does not give contractors adequate notice of the changed requirements or adequate implementation time.

2. \textbf{A Government-Wide Uniform Standard Is Needed.}

The Section supports NIST’s effort to develop a uniform standard for nonfederal systems with CUI and concurs that adopting a uniform government-wide standard serves the interests of both the Government and industry much better than imposing myriad varying and potentially costly, duplicative, or conflicting controls. Such harmonization is consistent with the Cybersecurity Executive Order that requires acquisition regulators to

\textsuperscript{22} DFARS 252.204-7012(a)(defining “covered contractor information system”).
\textsuperscript{23} DFARS 252.204-7012(b)(1) (Nov. 2013). Table 1 details the applicable controls.
\textsuperscript{24} 78 Fed. Reg. 69273, 69278 (Nov. 18, 2013).
\textsuperscript{25} Id.
\textsuperscript{26} NIST Publishes Final Guidelines for Protecting Sensitive Government Information Held by Contractors, NIST Tech Beat (June 19, 2015), \url{http://www.nist.gov/itl/csd/20150618_sp800-171.cfm}.
\textsuperscript{27} NIST SP 800-171, at 2 n.7 (indicating that the CUI regulation is “[p]roposed 32 CFR Part 2002, projected for publication in 2015”).
\textsuperscript{28} Id. at 35.
“address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.” 29 Such harmonization would also serve other fundamental principles governing federal acquisitions and cybersecurity needs, including regulatory consistency, cost-effective cybersecurity, greater competition, and enhanced security.

Harmonizing security controls, wherever possible, enhances 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, the forthcoming 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.” 30

The Section is concerned, however, that the interim rule could undermine the benefits of harmonization. DoD issued the prior UCTI rule only two years ago. The interim rule would now impose new and different requirements on contractors’ internal systems, before NARA completes its efforts under the Executive Order. The Section is particularly concerned about the impact of the interim rule’s change to the technical baseline for “adequate security” for a second time within such a short period. Moreover, defense contractors are likely to find themselves contractually required to meet the security requirements of the prior UCTI rule and the interim rule for the same information systems at the same time. The issuance of an interim rule without prior notice and coordination with the defense contracting community and the commercial contractors who provide services and products to the Government creates confusion and uncertainty that could undermine the conduct of full and open competition and the benefits of harmonization.

3. **The Lack of an Implementation Period To Achieve Compliance with Requirements Is Impractical.**

Contractors must expend significant effort to implement the controls necessary to strengthen network defenses in individual companies, no less throughout a multi-tiered supply chain covering thousands of large businesses, small businesses, and commercial providers. 31 The implementation of new cyber measures in any company cannot be accomplished within a one-day transition period, but instead takes time, money, and

---

30 NIST SP 800-171 at vi.
31 As described below, on October 8, DoD recognized a significant challenge faced by many contractors as to a particular control and issued a class deviation replacing DFARS 252.204-7012 and 252.204-2008 with revised clauses that gave covered contractors up to nine (9) months (from the date of contract award or modification incorporating the new clause(s)) to satisfy the requirement for “multifactor authentication for local and network access” found in Section 3.5.3 of NIST SP 800-171.
cyber and IT resources that are increasingly in short supply in public and private sectors. Simply stated, the interim rule does not provide a notice or implementation period and the associated practical difficulties to comply could undermine DoD’s laudatory objective.

To appreciate and understand the challenges and complexities associated with implementing and maintaining information systems with detailed security controls, the federal Government’s own experience with FISMA compliance is instructive. Thirteen years after the enactment of FISMA and years after the release of the original version of NIST SP 800-53, federal agencies continue to struggle to implement adequate information security controls against the evolving cybersecurity threat landscape. In fact, the General Accountability Office in a report just published in September 2015 found that government compliance remains far from complete.32

An immediately effective interim rule is inconsistent with recent experience in the challenges in implementing effective cybersecurity controls and inconsistent with the rules that apply to federal agencies’ systems when NIST identifies new security controls. The interim rule requires contractors to comply with the version of NIST SP 800-171 “that is in effect at the time the solicitation or as authorized by the Contracting Officer.”33 In contrast, federal agencies typically have one year to achieve compliance on legacy systems with NIST publications.34 Such a transition period is equally appropriate for federal contractors and the commercial supply chain supporting such agencies. The Section recommends modifying the interim rule to provide contractors a reasonable transition period of at least one year to implement any security controls not required by the prior UCTI rule and to implement any future changes to NIST SP 800-171. The Section submits that if there are particular contracts for particular systems or types of information that require more accelerated compliance periods, then those might be covered in a separate and specific requirement. Requiring all contractors at all tiers to comply with brand new requirements immediately is unfair and unrealistic.

---


33 DFARS 252.204-7012(b)(1)(ii)(A).

34 See https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf for a copy of the November 2013 Office of Management and Budget (“OMB”) memorandum instructing heads of executive departments and agencies as to FISMA reporting requirements. The response to Question No. 13 in the attachment entitled “Fiscal Year (FY) 2013 Frequently Asked Questions on Reporting for the Federal Information Security Management Act and Agency Privacy Management” provides: “For legacy information systems, agencies are expected to be in compliance with NIST standards and guidelines within one year of the publication date unless otherwise directed by OMB. The one year compliance date for revisions to NIST publications applies only to the new and/or updated material in the publications.”
4. NIST SP 800-171 Imposes Significant New Controls on Covered Contractor Information Systems.

The preamble to the interim rule states that “NIST SP 800-171 greatly increases the protections of Government information in contractor information systems, while simultaneously reducing the burden placed on the contractor by eliminating Federal-centric processes and requirements currently embedded in NIST SP 800-53.” The preamble further suggests that “a task analysis comparing the requirements of NIST SP 800-171 to the current table of security controls (based on NIST SP 800-53) demonstrates a reduction in required tasks by 30 percent.” There are, however, no additional details or data about this task analysis or the estimated reduction, and a review of NIST SP 800-171 itself suggests the interim rule imposes material new obligations on contractors’ internal systems with covered defense information.

In fact, the standard being imposed on nonfederal systems, NIST SP 800-171, even includes one derived requirement that does not yet fully apply to DoD or other federal agencies. Under the interim rule, covered contractor information systems must meet derived requirement 3.5.4, which requires such internal systems to “[e]mploy replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.” NIST SP 800-53, however, does not now require replay-resistant mechanisms for non-privileged accounts. A footnote in NIST SP 800-171 acknowledges this discrepancy and states this particular requirement will not be added to NIST SP 800-53 until its next update.

DoD has already taken remedial action regarding one of the material new requirements imposed by the interim rule. On October 8, 2015, DoD issued a class deviation to address one of the derived requirements, multifactor authentication. This requirement mandates that contractors use “multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.” When multifactor authentication is required, a user name and password alone may no longer be used to sign on to a system. Instead, a user authenticating to a network must have two or more different factors. Possible factors are (i) something the

---

36 Id.
37 See NIST SP 800-171, Appendices D and E. The traceability appendices in NIST SP 800-171 suggest that this new set of NIST requirements are traceable, at least in part, to more than 75 previously inapplicable NIST SP 800-53 security controls. Many of the controls are also not traceable to the more commercially used ISO/IEC 27001 standard.
38 See NIST SP 800-171 at 11.
39 Id., Appendix D at D-10 n.28.
40 A copy of the class deviation (DAR tracking number 2016-O0001) is available at http://www.acq.osd.mil/dpap/policy/policyvault/USA005505-15-DPAP.pdf.
41 See NIST SP 800-171 at 11 (§ 3.5.3) (emphasis added).
user knows, such as a password; (ii) something the user has, such as a token or a badge; or (iii) something unique to the user, such as a fingerprint or other biometric data.42

This multifactor authentication was not a requirement that had been imposed by the prior UCTI rule. Nor is this requirement fully implemented on government systems.43 With the class deviation, DoD modified both the interim versions of DFARS 252.204-2008 and 252.204-2012 to allow contractors, upon request to the contracting officer, up to nine months to become compliant with the multifactor-authentication derived requirement.44

The Section supports the class deviation but believes more relief is necessary to allow contractors to meet the new challenges imposed under the interim rule. Multifactor authentication is only one of the new NIST SP 800-171 requirements imposed by the interim rule without any transition period.

Even the largest contractors with sophisticated information security programs may not be compliant with the full set of NIST SP 800-171 requirements. This immediate implementation, however, will have a disproportionately adverse impact on small and mid-sized contractors. For small and mid-sized companies with less mature cybersecurity measures in place and potentially less in-house cybersecurity expertise, compliance will not be achieved without a significant expenditure of costs, time, and resources, much of which will come from external sources. These contractors need to start by obtaining the technical cybersecurity expertise to understand the requirements and potential compliance alternatives. Achieving compliance will require careful planning of changes to their internal information technology capabilities, not to mention budgeting for those changes. The Section therefore recommends that DoD establish an implementation period of at least one year for achieving compliance with NIST SP 800-171 as a whole, and provide additional relief to small and mid-sized businesses.

C. **The Section Applauds Including a Right to Propose Alternative, Equally Effective Controls, But Is Concerned that the Lack of Detail About the Process May Raise Implementation Concerns.**

The Section applauds DoD’s including in DFARS 252.204-7008 and 252.204-7012 the right to propose “alternate but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.” Under the interim rule, such requests to provide alternate methods of

---

42 Id. at 11, n.22.
43 See 2015 GAO report at 24-25 (noting that the 24 agencies covered by the Chief Financial Officer’s Act of 1990 have achieved a combined 72% implementation of these requirements (versus a 75% government wide goal). This number dropped to only 41% implementation for the 23 civilian agencies). DoD itself slipped two percent in its multifactor authentication progress from 89% to 87% during fiscal year 2014. Id. at 20.
complying with NIST SP 800-171 must be approved in writing by an authorized representative of the DoD CIO before contract award. The ability to propose such alternative control methods is consistent with Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” and the NIST Cybersecurity Framework, which recognizes that there is no “one-size-fits-all approach” to cybersecurity. This flexibility is also consistent with the recognition in NIST SP 800-171 that nonfederal organizations have information technology infrastructures in place with specific safeguarding measures or could develop such infrastructure, which may also be sufficient to satisfy the CUI security requirements.

The Section fully concurs with these assumptions and agrees that DFARS 252.204-7012 must continue to include a process permitting contractors to deviate from specified security controls or to propose alternatives to them. The Section also believes that including review and approval of these requests by DoD’s CIO (versus review by individual contracting officers under the prior UCTI rule) is a positive step that will help ensure consistency and fairness in competitions if properly implemented. That said, the Section believes DoD should provide additional transparency to the specifics of the process, ranging from the specifics of the submittal process to the standards to be used to approve or disapprove submissions. These concerns broadly fit into four areas.

First, the Section has several operational concerns about how this deviation-request process will work in practice. For example:

- Does DoD have sufficient personnel allocated to handle such requests from contractors during the proposal stage, including for short turn-around competitions?
- How does DoD intend to manage the relationship between acquisition personnel and the DoD CIO representative? Will contracting officers be serving in this representative role, or will this authority reside elsewhere?

The interim rule does not describe the operational realities of how this process will work in practice.

The ability of the DoD CIO office to process all of the submissions that may be made under DFARS 252.204-2008 promptly is essential because the interim rule precludes contract award until after the DoD CIO documents its determination. Although the Section recognizes that DoD need not delve into this level of specificity in the interim rule itself, we encourage DoD to provide more concrete guidance to both its internal stakeholders and the contractor community as to how it envisions implementing this critical process. The Section would like to further encourage DoD to consider modifying

---

45 DFARS 252.204-7008(d); DFARS 252.204-7012(b)(1)(ii)(B).
46 NIST SP 800-171 at 5.
the interim rule to establish a short timeframe in which the DoD CIO office must review and approve the submissions to avoid disruptions to the procurement process.

Second, the Section is concerned that the lack of specificity in DFARS 252.204-2008 will lead to an inconsistent treatment of requests for approval for alternative, equally-effective controls. The Section recognizes the need for flexibility and does not advocate rigidity of process over substance, but the Section does believe that consistency would be served by the publication of guidance on the criteria that will be used to determine whether a particular alternative control is “equally effective” and achieves “equivalent protection.” Such consistency is critical to maintaining a level playing field so that contractors can compete for DoD procurements on a fair and equal basis.

Third, the interim rule does not discuss how this process should apply to subcontractors. Whereas the interim rule permits direct access to DoD in some areas—such as self-reporting of incidents—it does not provide a similarly clear path for subcontractors wishing to propose alternative controls. Given the sensitivity of data regarding internal controls, subcontractors also may be reluctant to share this information with prime contractors, some of whom may be competitors in other procurements.

This concern raises another set of operational questions, the answers to which the Section believes are essential for effective implementation of the rule:

- Will DoD empower contractors to approve subcontractors’ requested deviations, or must prime contractors refer all such requests to DoD?
- Are prime contractors required to flow the deviation authority down to subcontractors?
- Does DoD have sufficient resources in place to assist with such requests for the full supply chain?

These open issues are complicated by companies’ often serving as prime contractors in some procurements and as subcontractors in others.

Fourth, given the security concerns over providing detailed information about specific controls on company’s internal systems, further clarity is needed as to how these submissions will be protected both within DoD and from public disclosure by the Government. The Section recommends that DoD permit companies at their option to submit any requests under DFARS 252.204-2008 directly to the CIO office.

The Section requests that DoD address these critical questions in the final rule to provide clarity for all levels of the supply chain.
D. The Scope of the Reporting Requirements Is Overbroad and Impracticable.

1. The Definitions Relevant to Cyber Incidents Should Be Clarified.

The interim rule requires reporting of cyber incidents affecting covered contractor information systems, covered defense information residing therein, or “the contractor’s ability to perform the requirements of the contract that are designated as operationally critical support.”47 A “cyber incident” is defined as “actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.”48 Once a cyber incident is discovered, contractors must both conduct a review for evidence of “compromise” of covered defense information and rapidly report (within 72 hours) the cyber incident.49 Compromise is defined as “disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized or unintentional disclosure, modification, destruction, or loss of an object, or the copying of the information to unauthorized media may have occurred.”50

The Section notes that some of the definitions carried over from the prior UCTI rule are ambiguous. For example, there is no definition for “security policy of a system,” which could reasonably equate with a breach of a firewall or other system control or, if broadly construed, any violation by an authorized user of a company information technology procedure (e.g., an employee emails from his or her work computer a nonproprietary document that is not CUI to his or her home computer). The Section believes that such an interpretation would result in over-reporting. Given the expansion of the interim rule and DoD’s and companies’ limited resources, the Section recommends that DoD, to the greatest extent possible, tailor its reporting requirements to appropriate contractors and subcontracts, and tailor subsequent follow-up activities to incidents that directly impact “defense covered information.”

The interim rule’s new application to cyber incidents that “affect the Contractor’s ability to provide operationally critical support” also is not clear. While the interim rule suggests that DoD will designate specific portions of its contracts that it considers to be operationally critical support,51 the scope of what constitutes a contractor’s “ability to provide operationally critical support” is so vague that it may not accomplish its purpose. Contractors may over-report and unnecessarily tax DoD’s compliance and cyber investigative resources, or they may interpret the clause too narrowly and therefore not

47 DFARS 252.204-7012(c)(1).
48 DFARS 252.204-7012(a).
49 DFARS 252.204-7012(c)(1).
50 DFARS 252.204-7012(a).
51 Id. (“Operationally critical support means supplies or services designated by the Government as critical . . . ”).
report actual cyber incidents. The Section suggests that DoD consider clarifying that a reportable incident occurs when a cyber incident affects the security or integrity of operationally critical information residing in a contractor information system.

2. **The 72-hour Reporting Window Is Impractical.**

The Section recommends that DoD undertake an analysis of the feasibility of the 72-hour reporting requirement. Contractors, especially small contractors who do not have large in-house information technology or information security departments, indicate that the 72-hour window is insufficient given: (i) the need to focus first on stopping and remediating any potential threat; (ii) the types of information required for reports; and (iii) the fact-finding and forensics investigation required to produce accurate information for reports.

The DoD-DIB Cyber Reporting web portal\(^\text{52}\) referred to in the interim rule requires companies to complete cyber incident reports with as much of the following information as possible:

1. Company name
2. Company point of contact information (address, position, telephone, email)
3. Data Universal Numbering System Number
4. Contract number(s) or other type of agreement affected or potentially affected
5. Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
6. Government Program Manager point of contact (address, position, telephone, email)
7. Contact or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
8. Facility Commercial and Government Entity (“CAGE”) code
9. Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
10. Impact to Covered Defense Information
11. Ability to provide operationally critical support
12. Date incident discovered
13. Location(s) of compromise
14. Incident location CAGE code
15. DoD programs, platforms or systems involved
16. Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
17. Description of technique or method used in cyber incident
18. Incident outcome (successful compromise, failed attempt, unknown)

\(^\text{52}\) http://dibnet.dod.mil.
19. Incident/Compromise narrative
20. Any additional information

To access the reporting site to provide the information, the contractor or subcontractor must have or acquire a DoD-approved medium assurance certificate.53

Generally, 72 hours is not enough time to investigate a potential cyber incident, confirm the incident, and obtain the requisite report information. For example, a security alert might indicate some unusual system activity that raises concerns. The contractor must undertake multiple concurrent steps to determine whether the alert is a false alarm or whether a compromise may have occurred. Contractor personnel will need to review various sources of information such as network and system logs, correlating events from other security systems, network topology, and other system information. Determination of the scope of the potential incident may entail review of multiple computers, servers, large forensic disk images, system accounts and remote devices tied to the system (which may not all be readily accessible). Even if a compromise is verified, identification of how the compromise occurred is similarly complex, as it may involve an analysis and investigation of multiple issues, including physical security, password protection practices on many computers, compensating security controls as well as the computer system itself. At the same time this review is ongoing, the contractor will need to implement measures to contain the incident, assess the impact, preserve its data and information, and preserve and image the affected system components.

Of even greater practical impact is the onus the interim rule appears to place on contractors and subcontractors to identify “covered defense information” on their information systems, even if such information is not marked as such by the Government or the Government fails to provide adequate marking instructions. The definition of “covered defense information” also presupposes a company’s knowledge of the ultimate source, use or purpose of the information on the contractor’s system—i.e., that the information was provided to the contractor by or on behalf of DoD, or is being collected, developed, received, transmitted, used or stored by the contractor in support of a particular DoD contract. Many companies have or have had hundreds of contracts and subcontracts and may not be able to trace a particular document, particularly if it is unmarked, with exact precision within hours. A lower-tier subcontractor may not know whether unmarked information originated from DoD or is being generated or used in connection with a DoD contract.

Accomplishing all of these activities within a 72-hour period is impracticable, as illustrated by recent data breaches reported by federal agencies. By way of comparison, most state personal information breach reporting requirements define the reporting time period as “without undue delay,” or provide significantly longer than 3 days to report an incident. The Section thus recommends DoD revisit the 72-hour reporting period and

53 DFARS 252.204-7012(c)(3).
perform an analysis of what is a realistic time period consistent with federal experience, other security regimes, and the nature of the data DoD is requesting.

3. **The Reporting Requirement Is Unworkable for Subcontractors.**

The interim rule requires subcontractors to report cyber incidents within the same 72-hour timeframe directly to DoD (using the same DoD central reporting portal) and the prime contractor.\(^54\) Thus, DoD expects subcontractors to file reports including such information as the affected DoD contract numbers and point of contact information for the DoD contracting officer or program manager, information few subcontractors are likely to have. As discussed above, a subcontractor will face even more difficulty in identifying or tracing the origin of covered defense information if it is not properly marked. DoD’s application of and enforcement of the interim rule should take into account the practical limits on effective subcontractor reporting posed by these informational deficits at lower levels of the supply chain.

4. **DoD Should Consider Clarifying Reporting Mechanics.**

DoD should also consider clarifying the mechanics of the reporting requirement when a single contractor information system contains “covered defense information” for multiple DoD contracts or programs. Indeed, depending on the nature and scope of an individual breach, a cyber incident could potentially implicate many—if not most or even all—of a contractor’s DoD contracts. For larger defense contractors, that could equate to hundreds or even thousands of individual contracts or orders.

The interim rule should be modified to specifically address which contracting officer will have the lead to act on behalf of DoD for purposes of directing the contractor’s further obligations in response to the cyber incident and any further cooperation required under the clause in the event multiple contracts are implicated in a single cyber incident. Having multiple DoD contracting officers providing a contractor with potentially different instructions would burden both DoD and contractor resources unnecessarily, contrary to the FISMA policy of cost-effective security. DoD instead should speak with one voice in, for example, instructing a contractor to provide access to additional information or equipment or declining interest in the contractor’s preserved media/data, by establishing procedures under which DoD would designate the “cognizant contracting officer” to represent DoD in further investigation/assessment of the incident.

The FAR recognizes such an approach—with one contracting officer acting officially on behalf of the Government for multiple affected contracts—in other contexts, such as in approval of change of name or novation agreements under FAR Subpart 42.12 or the negotiation of final indirect cost rate proposals under FAR Subpart 42.7. The Section believes such an approach is warranted here as well.

---

\(^{54}\) DFARS 252.204-7012(m).
5. The Interim Rule Creates the Potential for Collateral Regulatory and Enforcement Consequences of Imposing Mandatory Reporting on Contractors.

The Section notes that certain categories of covered defense information, such as export-controlled information, may not as a matter of law be governed or managed by DoD itself. As such, the Section recommends that the final rule clarify that any assessment of the consequences of a disclosure of such categories of covered defense information should remain within the province of the agency designated by law for the information (in the case of the ITAR, the State Department, or the EAR, the Commerce Department), and should be an independent matter for the contractor or subcontractor to assess and report upon as appropriate to that agency. In addition, the final rule should clarify that mandatory rapid cyber incident reporting does not obviate any protections afforded by such regulating agency’s voluntary disclosure programs.

E. DoD’s Access/Use/Disclosure Rights to Company’s Internal Systems and Data Are Overbroad and Inconsistent with Cost-Effective Security.

The interim rule requires contractors to both preserve and make available extensive data from their internal systems. Specifically, DFARS 252.204-7012 mandates:

(e) Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

Thus, under this clause, if an employee’s laptop were potentially compromised (e.g., through a spear phishing campaign or otherwise) and the laptop included some “covered defense information,” an image of the laptop would need to be made and, upon request, provided to DoD (or a third party contractor). This requirement on its face would apply even if the employee were a company accountant, human-resources professional, or lawyer.
As discussed more fully below, the Section recommends that the interim rule be revised to recognize the need for appropriate limits on the Government’s rights to request, use, and disclose sensitive contractor information to which it may obtain access as a result of a reported cyber incident or investigation.

1. **The Interim Rule Conflicts with Clear Congressional Intent by Omitting a Mechanism to Limit Data Provided to DoD.**

Notably absent from the interim rule is any mechanism by which the reporting contractor or subcontractor can raise concerns about, object to, or limit the data being provided due to its sensitivity. In contrast, the prior UCTI rule clearly provided “the requirement to share files and images exists unless there are legal restrictions that limit a company’s ability to share digital media. The Contractor shall inform the Contracting Officer of the source, nature, and prescription of such limitations and the authority responsible.”

This omission is inconsistent with a legislative mandate to address this important issue. Although Section 941 of the National Defense Authorization Act (“NDAA”) for Fiscal Year 2013 did require certain contractors to provide DoD access to covered systems for the purpose of determining whether and to what extent DoD information may have been compromised during a cyber incident, Congress instructed DoD that its resulting regulation must:

(B) provide that a cleared defense contractor is only required to provide access to equipment or information as described in subparagraph (A) to determine whether information created by or for the Department in connection with any Department program was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated; and

(C) provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person.

The Fiscal Year 2013 Joint Conference Statement for this provision not only emphasized Congress’ expectation that “DoD [would] consult with industry as it develops the reporting process” but also stated that the resulting DoD procedures should allow contractors “to remove proprietary or other types of information before DOD forensics teams copy information or ‘image’ systems.” The Fiscal Year 2015 NDAA provision

---

addressing operationally critical contractors contained almost identical language in reiterating the need for DoD to specifically address these issues.  

2. **DoD Access Should Be Subject to Appropriate Limitations.**

   The interim rule also does not adequately put limits on the circumstances under which, and the extent to which, DoD may access internal contractor system data. DFARS 204.7302 (a)(1)(iii) merely states that it is DoD “Policy” that contractors “will provide adequate security to safeguard defense information” and that contractors and subcontractors are required to submit to DoD media or access to covered contractor information systems and equipment upon request. This submission and/or access requirement is not expressly tied to any associated triggering event or limitation. In the implementing contract clause, however, DoD’s rights appear more limited. Subsection (e) of DFARS 252.204-7012 imposes an obligation to preserve media once a contractor determines that “a cyber incident occurs.” Similarly, DoD is permitted to seek “access to additional information or equipment that is necessary to conduct a forensic analysis” after a cyber incident occurs.

   The Section recommends that DoD clarify the interim rule in two ways. First, the final rule should clarify that the Government will request a contractor’s media only in connection with the Government’s investigation or assessment of a contractor report of a “cyber incident.” Second, consistent with the underlying statutory authority, the final rule should limit the extent of the data to be sought, such as by indicating that the Government may require access to equipment or information only “to determine whether information created by or for the Department in connection with any Department program was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated.” This revision would reconcile the two sections of the DFARS and should encourage a narrowly focused, need-to-know request/submission process instead of a broad-spectrum approach that may result in costs and risks to data or media unrelated to DoD business or unaffected by the incident.

3. **The Interim Rule Should Address How DoD Will Safeguard Any Contractor Data Provided.**

   The Section has additional concerns as to how media will be secured and protected once in DoD’s possession. The interim rule acknowledges, “information shared by the contractor under these procedures may include contractor attributional/proprietary information that is not customarily shared outside of the company, and that the unauthorized use or disclosure of such information could cause substantial competitive harm to the contractor that reported the information.”

---

59 DFARS 252.204-7012(e).
60 DFARS 252.204-7012(f).
61 DFARS 204.7302(c).
Accordingly, contractors have valid concerns regarding how the media and/or data provided under the interim rule will be safeguarded.

The interim rule states only that the Government “will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.” 62 Additionally, the interim rule does not address whether the Government will permit contractors any recourse should their data be improperly used, released or stolen from the Government’s possession. Given the acknowledged sensitivity of the data to be furnished by contractors, and reported problems with the Government’s own databases and systems security, the Section recommends that, as contemplated by Congress, DoD engage industry to establish and specify the security standards in place and the safeguards implemented to protect the contractor’s data and technology, and the recourse for contractors in the event of a breach of those safeguards.

4. **The Interim Rule Should Set Appropriate Limits on the Government’s Disclosure/Use Rights.**

As discussed above, after a cyber incident, DoD may obtain access to internal contractor and subcontractor data it otherwise would not. The Government’s rights to use and disclose such data should be narrowly tailored. The interim rule appears to expand the Government’s use and disclosure rights beyond those permitted under the prior UCTI rule or that are necessary for DoD’s purposes.

Under the prior UCTI rule, the Government was authorized to “use information, including attribution information and disclose it only to the authorized persons for purposes and activities consistent with this clause.” 63 The prior UCTI rule further stated:

> Nothing in this clause limits the Government’s ability to conduct law enforcement or counterintelligence activities, or other lawful activities in the interest of homeland security and national security. The results of the activities described in this clause may be used to support an investigation and prosecution of any person or entity, including those attempting to infiltrate or compromise information on a contractor information system in violation of any statute. 64

The interim rule, however, potentially expands DoD’s use/disclosure rights and creates a new distinction between information “created by or for DoD” and that which was not.

In particular, the interim rule provides:

---

62 DFARS 252.204-7012(h).
63 DFARS 252.204-7012(e).
64 DFARS 252.204-7012(f).
(i) Use and release of contractor attributional/proprietary information not created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

(1) To entities with missions that may be affected by such information;
(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;
(3) To Government entities that conduct counterintelligence or law enforcement investigations;
(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or
(5) To a support services contractor (“recipient”) that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) Use and release of contractor attributional/proprietary information created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government’s use and release of such information.\footnote{65 DFARS 252.204-2012(i)(j).}

The Section understands that the Government may have legitimate needs to use such data but is concerned that this new language is both ambiguous and unnecessary. First, the Section is unsure why the interim rule now distinguishes government rights in “information created by or for DoD” from “information not created by or for DoD.” The interim rule also does not define what is meant by information created by or for DoD. Second, the Section believes that authorization to release company information not created for DoD “to entities with missions that may be affected by such information” is too broad and could be used inappropriately to authorize providing data for reasons wholly unrelated to cyber, counterintelligence, or national security to any other governmental entity. Third, the authorization to use information created for DoD for any lawful government purpose similarly is subject to potential misuse if “information created by or for DoD” is undefined. The Section recommends that the final rule use the same use and disclosure rights that were contained in the prior UCTI rule. To the extent
that the final rule continues to make a distinction between types of information, the Section recommends that the term “information created by or for DoD” be defined to apply only to contract deliverables or information otherwise delivered to DoD in performance of a contract.

5. The Requirement to Mark Images and Other Data is Not Practicable.

The interim rule places the primary burden on the contractor to mark the information it wishes to protect as “contractor attributional/proprietary.” Specifically, DFARS 252.204-7012(h) states that, “[t]o the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information.” This provision does not account for the separate obligation for contractors to image their internal information systems as they exist as of the time of discovery of a cyber incident, including documents that are internal to the contractor or otherwise not intended for release outside the company and therefore may not have been pre-marked with protective legends. The interim rule should address how contractors can protect previously-unmarked information while still complying with the requirement to preserve images of the information system as of the discovery of the cyber incident. Alternatively, the interim rule should enumerate what steps the Government will take to ensure that the absence of a marking on a document produced to the Government as part of the forensic image of the contractor’s internal information system will not be treated as determinative of the Government’s ultimate obligations to protect that information as contractor attributional/proprietary.

6. DoD’s Access May Have Unintended Legal Consequences.

The Section is concerned about the interim rule’s provision of an unlimited right to request information located on a contractor information system affected by a cyber incident. Under the interim rule’s requirement that the contractor preserve an image of the affected information system, a cyber incident could result in a contractor providing highly sensitive information that is of little or no value to the Government’s investigation, in that it provides no information about the cyber incident. Examples include payroll information, sensitive personal information such as social security numbers, attorney-client privileged communications or attorney work product, internal investigations, bid and proposal documents, research and development documents, and proprietary drawings and other documents. This requirement, and other unlimited access provisions, such as the requirement to provide DoD with access to additional information or equipment necessary for forensic analysis or to provide all the damage assessment information gathered during its own assessment, may have unintended legal implications.

For example, the covered defense information system could include attorney-client privileged information or attorney work product. The production of an image including such data could potentially result in an argument that the company waived privilege. Companies that are assessing and analyzing cybersecurity breaches may find
themselves facing potential investigations or regulatory actions by a number of federal and state regulators, as well as private litigants. As a result, many companies may take the reasonable precautions to perform their forensics investigations under the supervision of counsel to preserve attorney-client privileged information and attorney work product. The Section recommends that the final rule address this issue specifically by providing a mechanism (as the prior UCTI rule did) for contractors to address these and similar issues with DoD, and clarifying that DoD access does not result in a waiver of any right or privilege.

The interim rule should also address personal information in internal contractor systems. A request for system data has the potential to conflict with privacy rights both in the United States and in foreign countries. For example, companies may need the consent of certain of its non-US employees to provide certain personal information to DoD. In light of recent decisions on the transfer and treatment of data between the European Union and other countries, including the United States, this poses a significant dilemma for contractors. The Section recommends that the DoD Privacy Officer review the interim rule and conduct a privacy impact assessment, and that DoD address special procedures and protections for personal information.


The interim rule may require a contractor to provide highly sensitive information after a cyber incident. For instance, DFARS 252.204-7012(c) specifies that a contractor may be required to provide “images of all known affected information systems identified in paragraph . . . and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report” to a government-support contractor. DFARS 252.204-7009, however, lacks the protections normally afforded to contractors where sensitive information is provided to such contractors under DFARS 252.227-7025, including the right to require a non-disclosure agreement. Having such protections is important to ensuring that sub-tier and/or commercial suppliers will accept this clause in their contracts because non-disclosure agreements are customary in the commercial marketplace. The Section believes that the provisions of DFARS 252.204-7009 should be revised to be consistent with 10 U.S.C. § 2320(f)(2) and DFARS 252.227-7025.

The interim rule should also clarify the procedures under which contractor information will be released and afford contractors the ability to object to the release of particular information (even if unmarked)—akin to a provider’s rights to object to the release of information under a Freedom of Information Act request. The interim rule provides for only after-the-fact recourse for a release that may have already inflicted potentially irreparable harm on the contractor.
F. **Third Party Support Contractor Access to Other Contractors’ Internal Systems Raises Serious Concerns.**

Although the Section recognizes that DoD—like industry—faces substantial difficulties in hiring and retaining limited cyber resources, the Section has identified three concerns associated with DoD’s stated intention to rely on support services contractors for review of internal company networks and the adequacy of the protections for contractor information. Specifically, the interim rule states in the revised DFARS 204.7302 that DoD may have such contractors “directly supporting Government activities related to safeguarding covered defense information and cyber incident reporting.”

First, the interim rule provides no limitations on the DoD’s ability to share information with third-party contractors. The interim rule purports to limit the access to activities related to cyber incident reporting or safeguarding covered defense information (such as forensic analysis or damage assessment services) but, at the same time, also includes a catch-all for any “other services that require data from another contractor.” Given the potential for such incident reports to contain competitively sensitive information, the interim rule would benefit from safeguards for such data in the hands of third-party contractors. Such safeguards and limitations are particularly important, given that the protections of the Trade Secrets Act (18 U.S.C. § 1905) are focused upon government personnel, rather than private-sector employees.

Second, although DoD has implemented a clause imposing restrictions on third-party rights for data obtained during the performance of such contracts, concerns remain regarding the effectiveness of such provisions. The addition of a new clause—DFARS 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information—imposes a confidentiality obligation upon receiving contractors and also includes generic penalties for unauthorized disclosure. Still, the clause does not address the measures needed to mitigate any potential conflicts of interest stemming from such third-party access.

Third, the third-party beneficiary right granted under DFARS 252.204-7009 may be inadequate to protect the reporting party’s interests. The clause suggests a potential federal cause of action against the support services contractor, but does not provide an effective avenue to enforce that right because there is no obligation under the clause to notify the reporting contractor that DoD has given the information to a third party. The Section agrees with the need for such a third-party beneficiary right, but also encourages DoD to incorporate an effective mechanism to notify the originating party about third parties with access to such data, as well as any disclosure of such data by those third parties.

---

66 DFARS 204.7302(e).
G. The Interim Rule Should Address Subcontractor/Supplier Flowdown Obligations.

The interim rule’s requirement that DFARS 252.204-7012 be flowed down to subcontractors and suppliers at all tiers, including commercial and commercial-off-the-shelf-item suppliers, poses several practical issues for contractors. The interim rule includes challenging and government-specific cybersecurity and incident reporting requirements that many commercial suppliers (particularly those for whom defense-related procurements are only a small fraction of their overall business) will be unlikely to accept. The clause’s sweeping rights of DoD access to a commercial contractor’s internal information systems represent a particularly difficult challenge for flowing access requirements down to commercial subcontractors.

This raises the key question of whether DoD intends to prohibit a contractor or subcontractor subject to DFARS 252.204-7012 from using a subcontractor or supplier that refuses to accept the clause as a flowdown provision. If a prime contractor cannot use such a supplier, a large number of key commercial suppliers will likely become unavailable, thus potentially jeopardizing successful performance of DoD contracts or, at a minimum, substantially increasing contractor costs and pricing and imposing risks of delay in locating alternate suppliers.

The flowdown requirements under DFARS 252.204-7012 provide prime contractors no flexibility on flowdown obligations. Under the clause at paragraph (m), the contractor is required to “(1) [i]nclude the substance of this clause, including this paragraph (m), in all subcontracts, including subcontracts for commercial items; and (2) [r]equire subcontractors to rapidly report cyber incidents directly to DoD . . . .” This clause stands in contrast to the more focused approach to flowing down the requirements of DFARS 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information, and 252.239-7010, Cloud Computing Services. Under DFARS 252.204-7009(m), a contractor is required to include the substance of the clause in subcontracts “for services that include support for the Government’s activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items.” Under DFARS 252.204-7010(l), a contractor must include the substance of the clause in all subcontracts “that involve or may involve cloud services, including subcontracts for commercial items.” The Section recommends that DoD consider applying a similar approach to the flow down obligations under 252.204-7012. In so doing, the DoD would enhance consistency among the clauses concerning the safeguarding of covered defense information by imposing obligations in only those subcontracts for which covered defense information is necessary to complete the subcontract requirements.

Even if a prime contractor is successful in ensuring all of its own subcontractors and suppliers accept the flowdown of DFARS 252.204-7012, lower-tier suppliers or subcontractors will likely reject the flowdown. In such a case, the prime contractor would have fulfilled its own contractual obligation by flowing the clause down to its
subcontractors, and the prime contractor may not have visibility into lower levels of the supply chain. The Section recommends that DoD advise how contractors might address this situation, including explaining how DoD it intends to enforce flowdown of the clause beyond the first tier of the supply chain.

Another question raised by the flowdown requirements in DFARS 252.204-7009, 252.204-7012, and 252.239-7010 is whether the DoD considers Internet Service Providers (“ISPs”) to fall within the definition of “subcontractor” for purposes of flowdown obligations. In the final rule issued on Safeguarding Unclassified Controlled Technical Information, DoD, in response to a respondent’s question, clarified that an ISP or cloud service provider (“CSP”) constitutes a subcontractor in this context, and that the contractor is therefore responsible for ensuring that the subcontractor complies with the requirements of the rule within the scope of the rule.67 The interim rule expressly addresses the use of CSPs in performing contracts under which covered defense information may be handled by a prime contractor, but the rule does not refer to ISPs. The Section recommends that DoD clarify whether ISPs are also subcontractors in this context and, if so, clarify the flowdown obligations applicable to ISPs.

H. The Interim Rule’s Cloud Computing Requirements Need Additional Clarification and Would Benefit From Increased Harmonization with Current Requirements.

1. The Interim Rule’s Cloud Computing Security Requirements Depart from Existing Standards and Include Unclear Terms.

The interim rule provides that CSPs delivering cloud services in connection with a covered DoD contract must “implement and maintain administrative, technical, and physical safeguards and controls” for “Government data” that comply with the requirements of the then-applicable version of the DoD Cloud Computing Security Requirements Guide.68

As an initial matter, since 2011 the Government has used The Federal Risk and Authorization Management Program (“FedRAMP”) to impose uniform security standards and procurement processes that are designed to address the unique cybersecurity issues affecting cloud information systems. Authorization packages for cloud services have been certified by the Joint Authorization Board, which consists of high-level security experts from the Department of Homeland Security, DoD, and the General Services Administration. Importantly, in support of FedRAMP, the Federal CIO Council—in consultation with technical and policy experts from the Office of Management and Budget, NIST, and industry—has developed a selected set of standardized security controls for cloud services that was derived from NIST SP 800-53. These controls have

---


68 DFARS 252.239-7010(b)(2). The current version of the SRG is available at https://info.publicintelligence.net/DoD-CloudSecurity.pdf.
been used to assess the security of every commercial cloud information system that is currently being used to provide cloud-based services to the federal Government. The interim rule would impose different requirements. Harmonization of these requirements with the FedRAMP obligations is necessary and guidance as to how these two regulatory schemes will interact should be provided.

If the interim rule is not revised for consistency with the existing FedRAMP obligations, the new obligations imposed should be clarified. First, the interim rule invokes guidance that can be changed without notice, even after a contract is awarded. Such an approach may not permit contractors to appropriately plan and allocate resources. It also poses uncertainty as to requirements and thus could discourage potential contractors from participating in federal procurements.

Second, the interim rule requires that CSPs maintain “all Government data that is not physically located on DoD premises” within the “50 states, the District of Columbia, or outlying areas of the United States.” The interim rule does not define “DoD premises,” and it is unclear whether DoD considers DoD installations or other DoD real property located outside the United States or its outlying areas to be “DoD premises.” It also is unclear whether this requirement applies only to the physical computing infrastructure that is used to deliver cloud services (e.g., networks, servers, storage, applications) or whether it also applies to all CSP employees who provide services under the contract.

Similarly, the interim rule defines “Government data” as “any information, document, media, or machine readable material regardless of physical form or characteristics, that is created or obtained by the Government in the course of official business.” This definition is very broad, and may, for example, include purely private or commercial/proprietary information, as long as it was “obtained by the Government in the course of official Government business.” The clause does not define the term “Government,” nor does it describe the types of activities that are considered “official Government business.”

---

69 DFARS 252.239-7010(a). Notably, this requirement does not apply to “Government-related data,” which is defined as “any information, document, media, or machine readable material regardless of physical form or characteristics, that is created or obtained by a contractor through the storage processing, or communication of Government data.” Id. Government-related data does not include contractor’s business records (e.g., financial, records, legal records or proprietary data) “that are not uniquely applied to the Government data.” Id. The clause does not, however, provide guidance on how to determine whether a particular record is or is not “uniquely applied to the Government data.” Id.

70 DFARS 252.239-7010(a).
2. The Interim Rule’s Cyber Incident Reporting Requirements Do Not Account for Unique Cyber Reporting Limitations.

The interim rule requires CSPs to report “cyber incidents” that are “related to the cloud computing service provided” under the subject contract or subcontract.71 The phrase “related to the cloud computing service provided” is quite broad and could be problematic for CSPs that utilize the same resources (e.g., servers, networks) to manage both government and non-government data. The breadth of this requirement is compounded by its adopting DFARS 202.101’s definitions of “cyber incident” and “compromise,” both of which are very broad. Indeed, as noted above, compromise is defined to include a violation of the security policy of a system. In addition to the breadth of the definition, the reporting requirements do not address some of the unique concepts that apply to cloud computing.

The interim rule prohibits CSPs and their employees from “access[ing], us[ing], or disclos[ing]” government data unless specifically authorized by the terms of their contracts or orders issued thereunder. Similarly, by design, commercial agreements often include provisions that, among other limitations, prevent the CSP from accessing the customer information for any reason without the customer’s prior consent. As a result of these types of limitations, whether an incident impacts a particular customer’s data and whether there are additional reporting requirements is known only by the customer. Thus, the Section recommends that the interim rule include a two-step reporting process, allowing the customer whose data is being stored in the cloud the ultimate determination of any reporting obligations to the Government. In the alternative, incident reporting guidance already been established under FedRAMP, which could serve as appropriate guidance.

I. The Interim Rule Extends Beyond the Statutory Focus on Certain Contractors and Could Have a Deleterious Effect on Small Business and Commercial Contractors If These Issues Are Not Fully Considered.

1. The Interim Rule Extends Beyond the Statutory Mandate.

The interim rule to require contractor reporting on network penetrations and to implement DoD policy on the purchase of cloud computing services exceeds the statutory bounds under which it is being issued. In publishing the interim rule, DoD cited two statutory requirements as authorizations for the regulation: Section 941 of the 2013 NDAA and section 1632 of the 2015 NDAA. These laws, however, specifically limited the scope of the contractors affected. Section 941 of the 2013 NDAA applies only to “cleared” contractors, i.e., those contractors handling classified information. That statute provided: “The Secretary of Defense shall establish procedures that require each cleared defense contractor to report to a component of the Department of Defense designated by

71 DFARS 252.239-7010(d).
the Secretary for purposes of such procedures when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.” Section 1632 of the 2015 NDAA expanded the scope of the requirement only slightly to include not only cleared contractors but also “operationally critical” contractors. That statute, however, defined “operationally critical” contractors narrowly: “The term ‘operationally critical contractor’ means a contractor designated by the Secretary for purposes of this section as a critical source of supply for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.” The interim rule, however, applies to all DoD contractors.

2. DoD Should Consider the Full Impacts of the Rule on Small Businesses and Consider Amending or Postponing the Regulations for Small Businesses.

DoD’s conclusion that the interim rule “[m]ay have a significant economic impact on a substantial number of small entities” mandates preparation of a regulatory flexibility analysis.72 Among other items, this analysis must include a description of, and, where feasible, an estimate of, the number of small entities to which the rule will apply; a description of the recordkeeping and compliance requirements and the types of professional skills necessary to perform these requirements; and a description of alternatives that would accomplish the rule’s objectives while minimizing any significant economic impact to small businesses. This analysis must also consider the establishment of differing compliance or reporting standards or timetables for small entities, potential simplification of the requirements for small businesses, and the feasibility of an exemption for the rule or part of the rule for small entities.73

DoD’s discussion of the rule’s impact on smaller contractors does not explain how the agency reached its conclusions, and there is significant evidence that it has underestimated the number of affected entities, the scope of the regulatory burden, and the financial impacts of the interim rule. First, the analysis asserts, without explanation, that the rule does not duplicate, overlap, or conflict with any other federal rules, and that there are no alternatives that would mitigate the impact on small businesses.74 As noted above, there is an extensive framework of laws and regulations on this subject, and explanations and guidance on how these various provisions can or will work together is needed.

More significantly, based on industry input and publicly available information, DoD’s regulatory analysis estimates the number of small contractors affected by the

73 5 U.S.C. § 603(b) and (c).
74 80 Fed. Reg. at 51740.
interim rule and the average number of hours involved in complying with the reporting requirements.\footnote{Id.}

DoD estimates that there are 10,000 contractors falling within the rule’s coverage, and that less than half of these are small businesses.\footnote{Id.} The interim rule does not explain the derivation of this number, and does not specify whether DoD included subcontractors in its estimate. Based on publicly available information, DoD’s estimation of less than 5,000 small business contractors appears to be understated. On September 24, 2015, GAO released a report titled, “Defense Cybersecurity: Opportunities Exist for DoD to Share Cybersecurity Resources with Small Businesses.”\footnote{Government Accountability Office, \textit{Defense Cybersecurity: Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses}, Report GAO-15-777 (Sept. 2015), \url{http://www.gao.gov/assets/680/672724.pdf} (“GAO Small Business Report”).} It states that, in fiscal year 2014, DOD obligated approximately $55.5 billion to small business prime contractors at over 51,000 locations. This number, which is drawn from the Federal Procurement Data System-Next Generation, does not include subcontractors.\footnote{Id. at 2, n.6.} It does suggest that DoD’s estimate of less than 5,000 small business subcontractors affected by the rule is too low.

Similarly, a search of the USASpending database reveals that there were 512,601 DoD contract actions involving small businesses in FY 2015 alone. Even assuming that only half of these contractors handle “defense covered information” and are thus covered under the interim rule, and even if each of these contractors were responsible for 20 contracts in fiscal year 2015, the number of small business subcontractors would still be over 12,000. This number also does not include subcontracts awarded to small businesses.

DoD’s assessment of the financial and administrative burdens on small business contractors is similarly understated. The regulatory impact assessment contains an approximation of 4.15 hours necessary to complete a report of a cyber incident, and an expectation of 5.5 reports for each company.\footnote{80 Fed. Reg. at 51741.} The DoD analysis also states that an information technology expert “will likely” be required in order to fill out the required reports. This impact assessment is incomplete.

It does not include the time, cost, and expertise required to obtain a DoD medium-assurance certificate, which is necessary to submit a report. Contractors must apply for a certificate, and the root certificate assurances must be downloaded on contractors’ computers. It does not consider the time and resources needed to (i) evaluate a contractor’s cybersecurity measures and compare them to NIST SP 800-171, (ii) design, prepare/obtain and install any additional preventive measures, (iii) monitor and maintain the cybersecurity protections, (iv) review and update a contractor’s cyber practices, its
hardware and software, and its policies and procedures on a continuous basis,
(v) implement employee policies and training, (vi) investigate, confirm, report and
remediate cyber incidents, and (vii) develop and submit for DoD CIO approval
cybersecurity measures that do not meet NIST SP 800-171’s standards. It also does not
consider the cost to small businesses of having to review and revise their contracts with
subcontractors or third-party providers (such as CSPs).

DoD recognizes that an IT professional is necessary to complete the reporting
form, but it has not allowed for the continuing need for an IT professional or
professionals to implement any changes to computer systems; continue to monitor
operations; audit operations; or investigate, confirm, resolve, and report cyber breaches.
DoD appears not to recognize that small businesses will most certainly need to hire
outside consultants, such as legal and regulatory specialists, to assist them in
understanding and reconciling the various and competing cybersecurity requirements
applicable to government contractors now and those coming in 2016.\footnote{DoD’s conclusion
that the interim rule does not duplicate, overlap, or conflict with any other federal
rules is puzzling. Both OMB and NARA issued cybersecurity standards earlier in the year,
and both rulemakings promised 2016 changes to the FAR. Many small businesses will therefore
find themselves subject to overlapping and inconsistent cybersecurity requirements.}

Overlaying all of these increased costs is DoD’s growing reliance on lowest price
technically acceptable procurements. If a small business is performing and bidding on a
large percentage of such contracts, the financial strains on it will be exacerbated because
the additional costs imposed by the interim rule cannot be passed on to the customer.

In sum, the number of small businesses affected by the interim rule, and the scope
of the impacts, are likely greater than DoD’s estimates. In the absence of a clear
understanding of who is impacted and how they are impacted, DoD cannot fulfill its
regulatory obligation to consider the establishment of differing compliance or reporting
standards or timetables for small entities, the potential simplification of the requirements
for small businesses, and the feasibility of an exemption for the rule or part of the rule for
small entities.\footnote{5 U.S.C. § 603(b) and (c).}

DoD should develop a complete and supportable estimation of the impact of the
interim rule on the small business community, and then reassess whether there are viable
alternatives to the rule, whether exemptions to some or all of the requirements for small
businesses are justified, or whether small businesses should be subject to a longer or
phased schedule for implementation.

In addition to the lack of understanding concerning the rule’s impact on the
operations and finances of small businesses, the GAO Small Business Report identifies
gaps in the resources available to small businesses to assist them with understanding and
implementing cybersecurity requirements. Recognizing the general lack of resources

---

80 DoD’s conclusion that the interim rule does not duplicate, overlap, or conflict with any other federal
rules is puzzling. Both OMB and NARA issued cybersecurity standards earlier in the year, and both
rulemakings promised 2016 changes to the FAR. Many small businesses will therefore find themselves
subject to overlapping and inconsistent cybersecurity requirements.

81 5 U.S.C. § 603(b) and (c).
available to small businesses, the GAO Report recommended that the DoD Office of Small Business Programs identify and disseminate cybersecurity resources, such as training, workshops, and guidance documents to the small business community. DoD agreed with the recommendation, but still has not acted on it. This lack of assistance resources is still another factor mitigating in favor of making an accommodation to the small business community in connection with the interim rule.

DoD should consider undertaking one of the following courses of action:

- Exempt small businesses from the interim rule’s coverage.
- Exempt small businesses from the interim rule’s coverage pending DoD’s analysis of the true costs of compliance on small business.
- Formulate a different set of standards for small businesses.

3. **DoD Should Consider the Impact of Applying the Interim Rule to Commercial Providers Before Implementation.**

The interim rule extends to commercial providers. In fact, the new clauses and provisions of the interim rule are added to the list of solicitation provisions and contract clauses for the acquisition of commercial items at 212.301(f). While some of the data safeguarding and security requirements mandated by 252.204-7012(b) may overlap with more commercial information technology security standards, many do not. Indeed, commercial companies are much more likely to have used NIST’s own risk-based Cybersecurity Framework, which at its core allows commercial companies to select internal systems controls based on their own internal risk assessment.

Putting aside the mandatory security controls, the interim rule requires commercial providers to undertake some very un-commercial actions. These actions include: cyber incident reporting to DoD within 72 hours of discovery under 252.204-7012(c); submission to DoD of discovered and isolated malicious software under 252.204-7012(d); cyber incident media preservation and protection for DoD under 252.204-7012(e); allowing DoD access to information/equipment under 252.204-7012(f); providing to DoD cyber incident damage assessment information under 252.204-7012(g); and inclusion of contractor attributional/proprietary information under 252.204-7012(h), (i) and (j). These reporting requirements are triggered anytime “covered defense information” is on a system. The broad scope of the interim rule’s cyber incident reporting to include cyber incidents that result in a “potentially adverse effect” to such systems also is foreign to the commercial marketplace. Simply put, the cyber incident reporting requirements are extra-commercial mandates that, while capable of being performed by commercial sources, are not customarily available in the commercial marketplace.

82 80 Fed. Reg. at 51740.
In the legislative history of the Federal Acquisition Streamlining Act of 1994, Congress recognized that restrictive acquisition provisions could deny federal agencies’ access to technologies widely available in the commercial marketplace.\textsuperscript{83} As the first step to fix this problem, Congress directed federal agencies to acquire commercial items “to the maximum extent practicable” under acquisition policies that more closely resemble those found in the commercial marketplace.\textsuperscript{84}

In May 2015, Congress highlighted DoD’s need for the commercial marketplace to provide access to the latest commercial innovations and technology, and the risk that DoD’s acquisition procedures and audits could drive away the commercial sector and emerging technologies:

Even when the DOD has incorporated commercial components, it is often not nimble enough to refresh this technology and is left relying on obsolete commercial solutions for its major systems. The committee is concerned that a key reason for this situation is that polices, regulations, and processes within DOD make it difficult for many high-tech companies to collaborate and do business with the Department. The committee has heard from several companies, for example, that government acquisition and contracting regulations, cost accounting standards and audits, and intellectual property policies can be a major deterrent to working with DOD.\textsuperscript{85}

Here DoD is imposing substantial requirements that are not shown to be customary in the commercial marketplace. Consistent with the analogous concerns raised by Congress, the costs and burdens imposed by the interim rule may have two unintended consequences: (1) decreased availability of commercial items, as well as the commercial item vendors and suppliers willing to do business with DoD, particularly on fixed-price terms; and (2) increased costs for commercial items in the federal marketplace.

DoD should consider the impact of the interim rule on its access to commercial items and availability of sources for those items, particularly given the expansion of the rule to all systems with “covered defense information.” The full potential impact of the interim rule on commercial providers should be studied and quantified by DoD before implementation of the interim rule.

\textsuperscript{84} Pub. L. No. 103-355, § 8104(b), as reprinted in 1994 U.S.C.C.A.N. 3243, 3391. The statute governing DoD acquisitions establishes this same mandate. 10 U.S.C. § 2377(b); see also FAR § 12.101.
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,

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