Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Keeping Up With DOD Cybersecurity Compliance Demands

By **Susan Cassidy, Ian Brekke and Weiss Nusraty** (March 19, 2019, 4:13 PM EDT)

Susan Cassidy

Ian Brekke

Weiss Nusraty

On Jan. 21, 2019, Undersecretary of Defense for Acquisition and Sustainment Ellen Lord issued a memorandum focused on assessing contractor compliance with the Defense Federal Acquisition Regulation Supplement, or DFARS, cyber clause via audits of a contractor's purchasing system.[1] One intent of this guidance is to have the Defense Contract Management Agency, or DCMA, "validate, for contracts for which they provide contract administration and oversight, contractor compliance with the requirements of DFARS clause 252.204-7012."[2]

This would be done as part of a review of a contractor's purchasing system in accordance with DFARS 252.244-7001. Pursuant to this DFARS clause, contractors are required to provide adequate security on their internal networks to protect covered defense information, or CDI, and are required to flow down DFARS clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," to subcontractors without alteration.

On Feb. 26, 2019, the DCMA updated its Contractor Purchasing System Review (CPSR) Guidebook to incorporate requirements from the January 2019 memorandum. In particular, the "Supply Chain Management Process" outlined in Appendix 24 states that "[p]rotecting Controlled Unclassified Information is a critical aspect" of supply chain management.[3]

The guidebook assumes obligations that are beyond those imposed by the DFARS clause, presumably assuming that new requirements will be imposed contractually in the future.

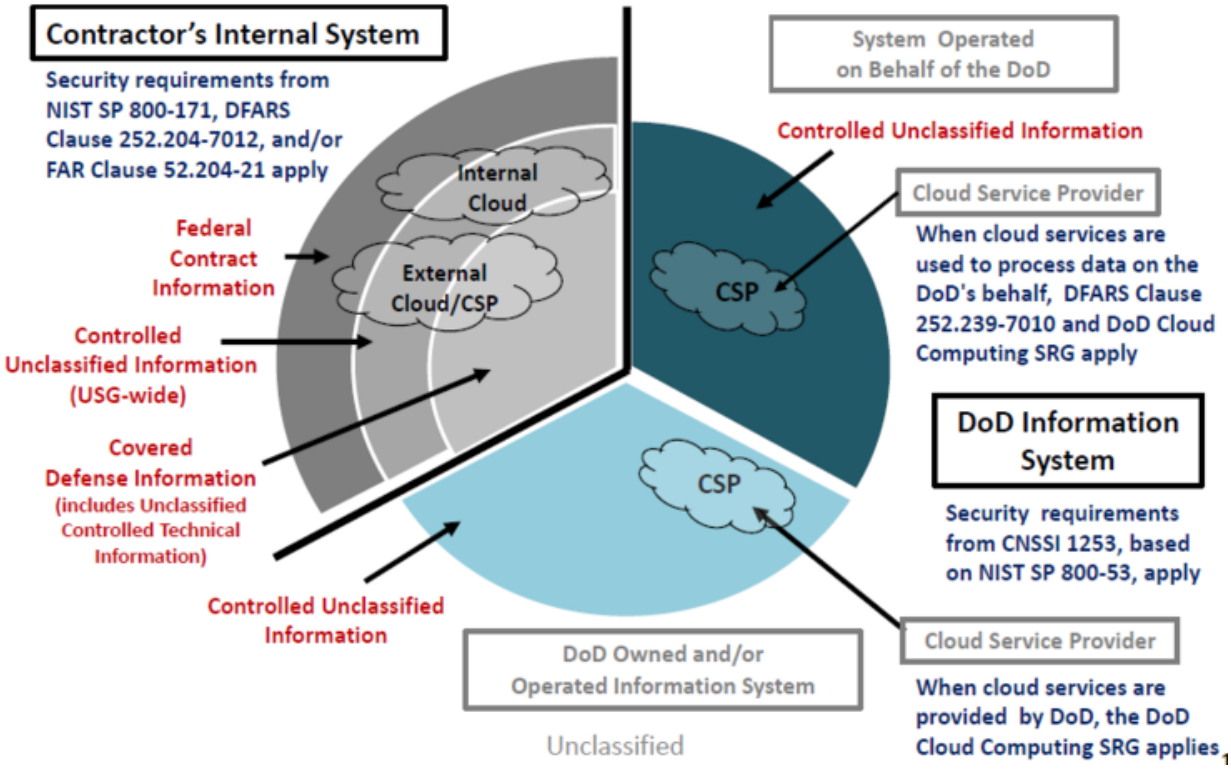
**Applicability**

The guidebook provides that if DFARS 252.204-7012 is applicable, the DCMA will evaluate a contractor's purchasing system to assess:

> (a) The contractor's procedures ensure contractual DoD requirements for marking and distribution statements on DoD Controlled Unclassified Information (CUI) flow down appropriately to their Tier 1 Level Suppliers.

(b) The contractor's procedures to assure Tier 1 Level Supplier compliance with DFARS Clause 252.204-7012 and NIST SP 800-171.

There are significant issues with both of these requirements. First, the DFARS clause addresses CDI, which is a subset of CUI. Thus, the DCMA appears to be auditing to a standard that is not reflected in the DFARS clause. Indeed, the Department of Defense has shown the below chart to industry many times depicting the narrower category of CDI versus CUI:[4]




Second, the guidebook assumes that the "DoD requirements for marking and distribution statements on DoD Controlled Unclassified Information (CUI)," actually exist. The definition and identification of CDI, both from a performance standpoint and now from an audit standpoint, remains one of the primary challenges for the DOD and its contractors.

In the Dec. 17, 2018, policy memorandum issued by Assistant Secretary of Defense for Acquisition Kevin Fahey, there was sample contractual language for requiring activities that covered identification and tracking of CDI flowed down to first-tier subcontractors, vendors and suppliers.[5] That sample contractual language, which refers to a post-award conference where the government and the contractor will "identify and affirm marking requirements" for all CDI and contemplates that the post-award conference will also address restrictions on unnecessary sharing or flow down of CDI, is now appearing in new solicitations.

Although the inclusion of a meeting to address the government's CDI marking requirements as a solicitation provision is a step in the right direction, by the time a post-award conference occurs, prime contractors will have already entered into teaming agreements and subcontracts with their supply chain without this knowledge. At that point, it may be too late for them to impose additional contractual

requirements on their team members. Moving this requirement to a pre-award time period may be a more useful process.

Finally, the guidebook's requirement to "assure Tier 1 Level Supplier compliance with DFARS Clause 252.204-7012 and NIST SP 800-171" is new. The DFARS clause provides that contractors must provide adequate security on their own covered defense systems[6] and that contractors must flow down the clause without alteration to subcontractors "if the information required for subcontractor performance retains its identity as covered defense information."[7]

Indeed, the DOD's own "Frequently Asked Questions" note that the requirement is to flow down the clause, not to assess compliance. Specifically, the DOD's current guidance is that "[i]f a subcontractor does not agree to comply with the terms of DFARS clause 252.204–7012, then covered defense information shall not be on that subcontractor's information system."[8] That obligation is contractual. By auditing whether contractors are "assuring" compliance by their Tier 1 subcontractors, the DCMA guidance exceeds the requirement that currently exists in the DFARS clause.

**During the Review**

The guidebook imposes additional significant requirements with regard to flowing down CDI — again, the guidebook continues to use CUI as the standard rather than CDI. For example, the guidebook imposes a tracking and assessment requirement. These requirements are reflected in the December 2018 policy memorandum but are not reflected in the DFARS clause. Moreover, the guidebook goes even further than the DOD December 2018 policy memorandum because it requires contractors to validate that all of their subcontractors' information systems "can receive and protect CUI."

Specifically, the guidebook states:

> The prime contractor must validate that the subcontractor has a Covered Contractor Information System (CCIS) that can receive and protect CUI. The prime contractor must show documentation that they have determined that the subcontractor has an acceptable CCIS to include an adequate System Security Plan (SSP).

There is no requirement in the clause for prime contractors to assess that a subcontractor's information systems are "acceptable," nor is that term defined by the DOD.

Similarly, there is no requirement in the DFARS clause for contractors to judge the adequacy of a subcontractor's SSP. Indeed, the DOD has told industry that there is no requirement for a third-party assessment of compliance on the part of prime contractors. For example, in the most recent version of the frequently asked questions issued by the DOD it states:

> Q15 (Q25): Is a 3rd Party assessment of compliance required?
>
> A15: 3rd party assessments or certifications are not required, authorized, or recognized by DoD. By signing the contract, the contractor agrees to comply with the terms of the contract.
>
> In order to safeguard covered defense information, companies with limited cybersecurity expertise may choose to seek outside assistance in determining how best to meet and implement the NIST SP 800-171 requirements in their company. But, once the company has implemented the requirements, there is no need to have a separate entity assess or certify that the company is compliant with NIST SP 800-171.[9]

Although the DOD has made it clear that it is relying on self-assessments for its prime contractors, it would now impose an assessment requirement on prime contractors for all of their subcontractors. This is a significant change in position by the DOD and does not reconcile the practical impediments to implementation, including that many contractors fill both the prime and subcontractor roles when working with the government.

Finally, the guidebook reflects two new "tracking" requirements: (1) to track cyber incidents reported by subcontractors and (2) to track subcontractor security requirement variance requests from NIST SP 800-171 made to the contracting officer.

Although the DFARS clause requires subcontractors to report to a prime that a cyber incident has occurred, it is unclear if the guidebook is imposing additional tracking requirements. Similarly, there is no requirement in the DFARS clause for tracking subcontractor security requirement variance requests, and the guidebook does not provide any explanation of what is required to meet this standard. Further guidance in these areas would be helpful for contractors.

**Impact on Contractors**

Just as the threat is evolving, the rules also are changing. Many contractors are becoming overwhelmed with new "guidance" for the DFARS clause. The continually revised guidance reflects that the DOD is also struggling with the threats and how best to protect its information.

Nonetheless, contractors should be aware of the new requirements that will likely show up in future contracts or modifications to existing contracts. The DCMA and industry may not agree that the DCMA's revised audit guidance is consistent with actual contractor obligations. Contractors should have a clear understanding of those requirements that actually fall within the DFARS clause and be careful to scrutinize any modifications and new solicitations for additional changes.

---

*Susan Cassidy is a partner at Covington & Burling LLP. Ian Brekke and Weiss Nusraty are associates at the firm.*



[1] "Addressing Cybersecurity Oversight as Part of a Contactor's Purchasing System Review," Memorandum, Ellen Lord, Under Secretary of Defense for Acquisition and Sustainment, Department of Defense (Jan. 21, 2019), available at https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19%20TAB%20A%20USD(AS)%20Signed%20Memo.pdf.

[2] Susan Cassidy & Ian Brekke, "DoD Continues to Up the Ante on Cybersecurity Compliance for Contractors," Inside Government Contracts Blog, Covington & Burling LLP (Jan. 29, 2019), available at https://www.insidegovernmentcontracts.com/2019/01/dod-continues-ante-cybersecurity-compliance-contractors/.

[3] Contractor Purchasing System Review (CPSR) Guidebook, Defense Contract Management Agency (Feb. 26, 2019), available at https://www.dcma.mil/Portals/31/Documents/CPSR/CPSR_Guidebook_022619.pdf.

[4] See Public Meeting on Network Penetration Reporting and Contracting for Cloud Services, Slideshow, Department of Defense (June 23, 2017), at Slide 16, available online at https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2017-06/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf.

[5] "Strengthening Contract Requirements Language for Cybersecurity in the Defense Industrial Base," Memorandum, Kevin Fahey, Assistant Secretary of Defense for Acquisition, Department of Defense (December 17, 2018), available at https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA003377-18%20ASD(A)%20Signed%20Memo%20w%20attach.pdf.

[6] DFARS 252.204-7012(b).

[7] Id. 252.204-7012(m)(1).

[8] Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73, DFARS Subpart 239.76 and PGI Subpart 239.76, FAQ REVISION, Department of Defense (April 2, 2018), available at https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2018-11/POSTED%20Revision%20to%20Cyber%20DFARS%20FAQs%20-%20April%202%202018%20rev%201.pdf, Q8 at 16.

[9] Ibid., Q15 at 17.