COVINGTON

Highlights of DoD Industry Information Day on the DFARS Cyber Rule

June 26, 2017

Government Contracts, Data Privacy and Cybersecurity

The Department of Defense ("DoD") held an "Industry Information Day" on June 23, 2017 at the Mark Center Auditorium in Alexandria, Virginia to address questions from Industry regarding DFARS Case 2013-D018 "Network Penetration and Reporting for Cloud Services," including DFARS clause 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting"(hereinafter "7012 clause") and 252.239-7010 "Cloud Computing Services" (hereinafter "7010 clause").

The presentation from the approximate four hour briefing is linked here and covered topics relating to DoD's expectations for contractor implementation of cybersecurity requirements for information systems and services that involve covered defense information ("CDI"). On the panel and responding to attendees' questions were representatives of DoD's Chief Information Officer, the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, and the Defense Information Systems Agency. Panelists were well prepared and receptive to questions from attendees, stressing the need for Industry and DoD to partner when it comes to protecting sensitive DoD data.

Although there were many topics covered during the briefing, this Alert covers some of the highlights and key learning points from the event. Release of a recording of the event is expected in the near future.

Highlights from DFARS Industry Day

DOD'S VIEW - Attendees were first greeted by Dr. John Zangardi, the Principal Deputy DoD CIO, who is currently serving as the Acting DoD CIO. Dr. Zangardi offered some insights into DoD's concerns. He noted that cyber incidents have surged by 38% since 2014, with the costs of those incidents estimated at $400 billion. Dr. Zangardi, as well as the panelists, noted that DoD needs assistance from its contractors to protect DoD's information and the Industry Day was an attempt to clarify DoD's needs and answer questions about implementation of DoD's cybersecurity requirements.

CHANGES TO THE DFARS RULE: At this time, DoD is not contemplating any changes to the DFARS clauses addressing cybersecurity. The next set of changes are likely to occur when the FAR version of the DFARS clauses are promulgated.

IMPLEMENTATION OF THE NIST SP 800-171 SECURITY CONTROLS: One question contractors have struggled with is whether the current compliance deadline of December 31, 2017 would remain in place or be extended to allow contractors extra time to complete their

implementation efforts. As noted above, DoD is not making any changes to the DFARS clauses and contractors are required to be compliant with the implementation of the NIST SP 800-171 (hereinafter "800-171") by the end of the year. Importantly, however, DoD clarified that "implementation" of 800-171 means having a System Security Plan ("SSP") and Plan of Action and Milestones ("POA&M") that accurately reflect the status of a contractor's compliance with the 800-171 security controls.

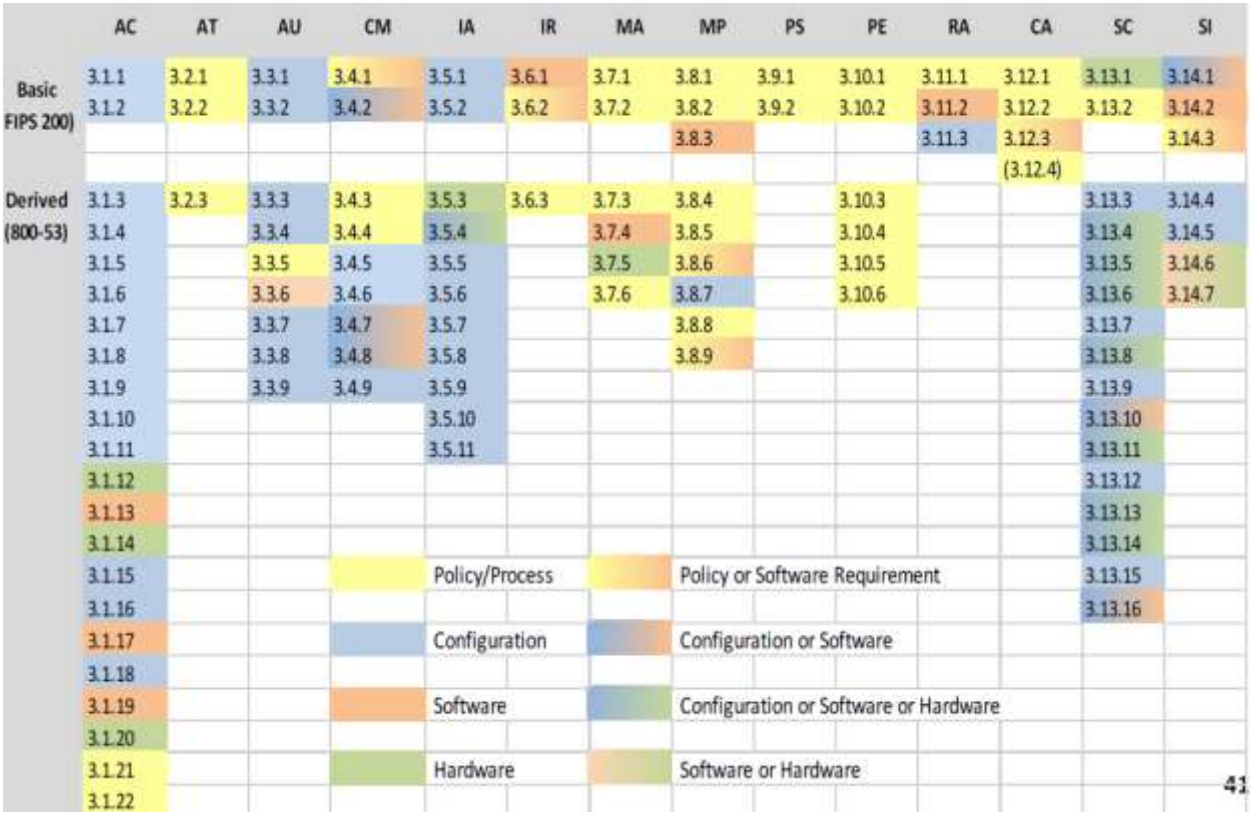
The panelists noted that under 252.204-7012(b)(2)(ii)(A), contractors are required to "implement 800-171, as soon as practical, but not later than December 31, 2017." Key to that implementation is the 110th security control that was added in Revision 1 to 800-171. This control requires contractors to create a SSP, which "describe[s] the boundary of [a contractor's]information system; the operational environment for the system; how the security requirements are implemented; and the relationships with or connections to other systems." NIST SP 800-171 Rev. 1 further notes that, if requested, contractors will be required to provide the Government with their SSPs and any associated POA&Ms. Moreover, federal agencies will be permitted to consider the submitted SSPs and POA&Ms as critical inputs when deciding whether to award a contract that requires the processing, storing, or transmitting of controlled unclassified information ("CUI") (or CDI for defense contractors) on a contractor information system.

The panelists clarified that if a contractor still has not implemented all 110 controls by December 31, 2017, but has a SSP and POA&M that accurately reflects the status of its compliance with those controls, that contractor has "implemented" 800-171 for the purposes of the 7012 clause. When pressed specifically as to whether the failure to notify a contracting officer ("CO") that some controls remain outstanding could be considered a violation of an implied certification for purposes of the False Claims Act, the panelists again stated that having a current and accurate SSP and POA&M reflecting the status of implementation of the 800-171 security controls would mean that the contractor has "implemented" the 800-171 controls as required by the 7012 clause, even if the CO has not requested a copy of the SSP or POA&M. This interpretation of the clause means that contractors would likely benefit from having the current version of the 7012 clause and Rev. 1 of 800-171 incorporated into their contracts.

Even with a current and accurate SSP and POA&M, however, it is possible that DoD could find that a contractor is not providing "adequate security," which is defined in the 7012 clause as "at a minimum" implementing 800-171 security controls. DoD may (or may not) accept the risks as defined in a contractor's SSP and POA&M. This finding could implicate both current contracts and proposals where safeguarding requirements are an evaluation factor. Thus, it is in contractors' interest to meet the full set of security controls as soon as practicable to avoid an impact on current and future DoD business. And, when the new FAR version of the 7012 clause is issued, this requirement for compliance is expected to extend across the Executive Branch.

THE PURPOSE OF THE 800-171 SECURITY CONTROLS: The panelists noted that one reason DoD moved from NIST SP 800-53 (hereinafter "800-53") to 800-171 security controls is that the 800-53 controls reflect both confidentiality and availability requirements for US federal agency systems. In contrast, the 800-171 controls are focused on maintaining the confidentiality of DoD information. Moreover, because 800-53 is directed at US Government information systems, the intent is to be consistent across the government. 800-171 is drafted at a much less granular level and permits more flexibility in implementation. This flexibility was reflected in a chart in DoD's presentation, which recognized that compliance can be achieved

through a combination of policies/processes, configuration, software, and hardware implementations. The chart from the presentation is set forth below and outlines the security controls required in 800-171 (the columns represent each of the 14 security control families and the values in each column represent the 800-171 control number).



CERTIFICATION OF COMPLIANCE: The panelists noted that by "signing the contract, the contractor agrees to comply with the terms of the contract," including the 7012 clause. DoD will not certify contractor compliance with the clause, nor will it accept certification from a third party assessor. The panel did note that companies without sufficient expertise in-house could use outside consultants to assist with self-assessments.

ALTERNATIVES TO 800-171 SECURITY CONTROLS: In some instances, contractors may want to implement security measures that provide protection equivalent to the controls defined in 800-171. In those cases, the DoD CIO will assess alternate measures based on a written submission from the contractor. The panel noted that the DoD CIO office works to provide assessment responses within five business days.

DCMA AUDITS: The panel confirmed that the Defense Contract Management Agency ("DCMA") will audit compliance with the 7012 clause. Among the points that DCMA will be focusing on are:

- Verifying that the contractor has a SSP;

- Verifying that the contractor submitted to the DoD CIO, within 30 days of any contract award made through October 2017, a list/notification of the 800-171 security requirements not yet implemented; and
- Verifying that the contractor possesses a DoD approved External Certificate Authority ("ECA") issued medium assurance public key infrastructure ("PKI") certificate.

If DCMA identifies (or is made aware of) a potential cybersecurity issue, DCMA will notify the contractor, DoD program office, and the DoD CIO. According to the DoD presentation, DCMA is also the government entity that would facilitate the entry of government external assessment team into a contractor facility for purposes of a damage assessment following a cyber incident. We are not aware of DoD having exercised this right with a contractor and the panel acknowledged that DoD likely can obtain the same information it requires from the preserved images of affected systems, which is already required under the 7012 clause.

DEFINITION OF CDI /CUI: Identifying what information qualifies as CDI/CUI remains a challenge for contractors. The panelists noted that DoD is still working to implement the NARA CUI Rule and documents are still being marked pursuant to DoD Instruction 5230.24 with one of seven distribution statements. The panelists noted that DoD is responsible for either marking information provided to contractors with one of those distribution statements or clearly stating in the contract how information provided under the contract should be marked. In its presentation, DoD cited to three areas in a contract where such identification should exist: (i) the statement of work ("SOW") (with a clear statement of how data should be treated per a distribution statement); (ii) Section I - contract clauses; and (iii) Section J - attachments. Most of this discussion was focused on guidance in the contract as to deliverables. What remains unclear is the determination as to data that is "[c]ollected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." *See* DFARS 252.204-7012(a). To the extent a contractor found a contract to be ambiguous on this issue, the panelists encouraged contractors to engage proactively with their COs to clarify which data under the contract might qualify as CDI. In response to attendee comments that COs often just responded by citing to the 7012 clause, the panel indicated that contractors also could reach out to the DoD CIO office for assistance.

When asked whether contract documents marked For Official Use Only ("FOUO") with no additional distribution statements would be considered CDI, the panelists noted that FOUO is a FOIA marking rather than a dissemination control. The panelists agreed that absent something in the contract limiting distribution of the contract itself, such contractual documents are unlikely to qualify as CDI. Similarly, the panelists noted that if a contractor is selling a commercial item with no modifications to DoD, then it is unlikely that CDI is required for contract performance. This may assist in determining whether a subcontractor providing commercial items under a non-Commercial Off-the-Shelf contract is subject to the 7012 clause.

SUBCONTRACTOR COMPLIANCE: The panelists stressed that a key message is that prime and higher tier contractors need to tailor and control what CDI data is provided to subcontractors to perform under the subcontract. It is the access to CDI by the subcontractor (whether flowed down or produced by the subcontractor during performance) that triggers compliance obligations for that subcontractor. It was the panelists' view that subcontractors are often given more data than necessary for performance, such as an entire technical package when the subcontractor is only providing one element of a deliverable. The panelists stated that tailoring flow down of data would better protect DoD's interests. The panelists agreed that if a

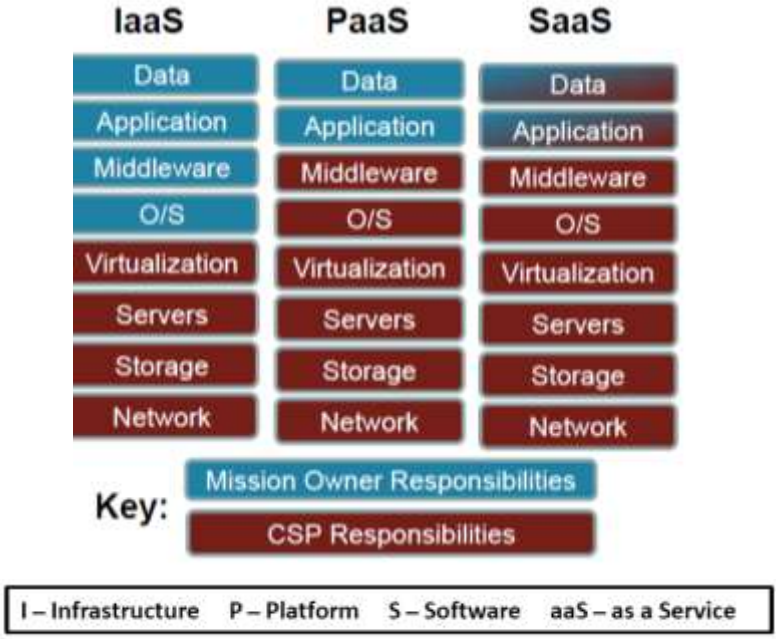
subcontractor cannot implement the required CDI protections, then CDI should not be shared with the subcontractor.

CLOUD COMPUTING: Some of the unique characteristics of cloud computing were recognized during the briefing.

7010 Clause vs. 7012 Clause: The panel clarified that the 7010 clause applies when a cloud solution is being used to process data on the DoD's behalf or DoD is directly contracting with a Cloud Service Provider ("CSP") to host/process data in a cloud. In this situation, the CSP steps into the shoes of DoD. This requires the CSP to comply with the DoD Cloud Computing Security Requirements Guide ("SRG") to include complying with the SRG's requirements for cyber incident reporting and damage assessment.

In contrast, the 7012 clause applies when a contractor uses an external CSP as an extension of its internal network and CDI is stored, processed, or transmitted by the CSP on the contractor's behalf. The contractor must confirm that the CSP meets requirements equivalent to those established for the Federal Risk and Authorization Management Program ("FedRAMP") Moderate baseline and complies with FedRAMP's requirements for cyber incident reporting and damage assessment. Significantly, DoD recognized that "[i]n most cases, the contractor will not actually 'flow down' the DFARS clause to the CSP, but must ensure, when using a CSP as part of its covered contractor information system, that the contractor can continue to meet the DFARS clause requirements, including the requirements in DFARS 252.204-7012 (c)-(g)." In other words, the CSP must agree to facilitate the contractor's obligations under the 7012 clause, but not necessarily comply with those requirements itself. If the CSP is considered a subcontractor for the contract effort and will be handling CDI on its own network outside the cloud environment, then the 7012 clause would flow down. DoD acknowledged that this would be atypical.

Differing Cloud Offerings: The panel acknowledged that the CSP's responsibilities will vary depending on the cloud service model being acquired and offered the following illustration in its presentation.



As this chart illustrates, DoD believes that a CSP's obligations to facilitate the contractor's responsibilities under the 7012 clause may vary depending on the type of cloud service being provided and the CSP's level of access to the contractor's data. If the CSP is FedRAMP and SRG certified it also may have independent reporting requirements under FedRAMP and the SRG for incidents at the infrastructure level.

Flow down of CDI: When asked whether CDI that is encrypted and provided to a CSP would qualify as the flow down of CDI to that CSP, the panel noted that if the CSP does not have access to the data (*i.e.*, cannot decrypt the data) then that data would not be seen as CDI. Consequently, the CSP would not be viewed as a subcontractor. That being said, the CSP must still agree to facilitate the contractor's obligations under the 7012 clause, but not necessarily comply with those requirements itself.

ADDITIONAL RESOURCES: DoD recognizes that it must provide its contractors certain resources to better understand the requirements for protecting the Department's data. DoD is currently working to update the following resources for its contractors:

- Frequently Asked Questions (which will be reorganized topically for easier use);
- Relevant Procedures, Guidance and Information ("PGI");
- Guidance to Stakeholders for Implementing DFARS Clause 252.204-7012, Safeguarding Unclassified Controlled Technical Information;
- FAR Case 2017-016, Controlled Unclassified Information; and
- DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems."

The DFARS cybersecurity requirements are complex and contractors should be diligent in confirming that they understand their obligations. This is especially true given that the FAR rule, which will apply across the entire federal government, is expected to be very similar to the current DFARS clauses.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our firm:

Susan Cassidy	+1 202 662 5348	scassidy@cov.com
Ashden Fein	+1 202 662 5116	afein@cov.com