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

Still Looking For Clarity In DOD Information Security Rule

By **Jeniffer De Jesus Roberts and Katherine Veeder**
(June 1, 2018, 12:51 PM EDT)

Jeniffer De Jesus Roberts

Katherine Veeder

The deadline to fully comply with the U.S. Department of Defense's requirements contained within Defense Federal Acquisition Regulation Supplement 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," to safeguard "covered contractor information systems" passed six months ago, on Dec. 31, 2017. Despite the passage of time, the DOD and industry are still struggling with what these information security requirements practically mean.

Agency procurement and contracting officials are trying to figure out their role in enforcing and monitoring implementation of the information security requirements. DOD prime contractors, on the other hand, generally understand whether the clause applies to them and what the clause requires, but they are wrestling with what noncompliance would mean and how they should apply the requirements to their supply chains. DOD subcontractors, for their part, are grappling with their own responsibilities under the clause. While the DOD issued some recent guidance in an effort to shed light in this area, many believe the rule remains as clear as mud.

DFARS 252.204-7012 — What Does It Require and When Does It Apply?

Under DFARS 252.204-7012, contractors must provide "adequate security" on all contractor information systems that process, store or transmit "covered defense information," i.e., unclassified controlled technical information or other information requiring safeguarding that is either (1) marked or identified as such and provided to the contractor in support of contract performance; or (2) "collected, developed, received, transmitted, used or stored" in support of contract performance. The rule explains that, at a minimum, "adequate security" means compliance with the 110 security controls contained in the National Institute of Standards and Technology Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." Importantly, the clause requires contractors to include DFARS 252.204-7012 in subcontracts for "operationally critical support" or subcontracts "for which subcontract performance will involve covered defense information, including subcontracts for commercial items."

After the promulgation of DFARS 252.204-7012, the DOD issued guidance providing that by the Dec. 31, 2017, deadline, contractors must either implement all 110 NIST SP 800-171 security controls or implement system security plans (SSPs) and plans of action (POAs) identifying the current state of compliance of their information systems and a plan to come into compliance within a reasonable period of time.

The Dec. 31 Deadline Has Come and Gone — Now What?

Months after the Dec. 31, 2017, deadline, questions continued to swirl regarding what, practically, implementation and enforcement of this clause would and should look like. To provide some answers, the DOD developed and on April 24, 2018, issued to the public for review and comment two forms of draft guidance.

The first, "DOD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented," is intended to aid DOD officials in the review and understanding of SSPs and POAs, establishing, among other things, "DOD Values" (effectively, risk ratings) to assess the impact of a contractor's unimplemented security requirement(s) as set forth in its SSP and POA. The second, the DOD's "Assessing the State of a Contractor's Internal Information System in a Procurement Action," sets forth the steps DOD officials can take in drafting a solicitation, evaluating proposals, and negotiating a contract so that DOD officials can meaningfully assess the state of a contractor's compliance with DFARS 252.204-7012 during the various stages of a procurement action. These two documents provide insight on the roles government officials will play in the enforcement of DFARS 252.204-7012 and the consequences the clause will have on DOD prime contractors and subcontractors alike.

Practical Implications for DOD Prime Contractors

First, contractors must realize that both DOD solicitations and contracts, except those solely for commercial off-the-shelf items, likely will contain or incorporate DFARS 252.204-7012 by reference. It will be critically important for contractors to flag this clause in their review of solicitations and contracts to confirm applicability to a particular contract.

Second, in order to give effect to these clauses, and once the DOD's guidance is finalized and implemented, contractors should expect more detailed compliance requirements in DOD solicitations and contracts relating to this clause, including:

- Contractors must submit with their proposals an SSP and POA together with notice that the government will either (1) evaluate the SSP and POA based on whether implementation of the NIST SP 800-171 controls is acceptable or unacceptable; or (2) evaluate implementation of NIST SP 800-171 as part of the government's technical evaluation using criteria set forth in the request for proposal.

- After contract award, the awardee must deliver an SSP or POA.

- The awardee during contract performance must periodically report the results of continuous monitoring.

- During contract performance, the government will monitor compliance with NIST SP 800-171, including using independent government assessments.

Third, DOD contractors should prepare to see one or more of the following in their contracts, particularly when covered defense information will be generated or provided:

- The incorporation either expressly or by reference of the contractor's SSP and POA into the contract.

- The inclusion in the contract's statement of work and contract data requirements list the requirement to deliver an SSP and POA, the requirement that the contractor implement a POA and/or that the government will track implementation of the POA.

- The inclusion of a requirement to periodically report on continuous monitoring results.

- The inclusion of a requirement to support any independent government assessment of the contractor's compliance with NIST 800-171.

These additions to solicitations and contracts will have a number of practical implications for DOD contractors. Because the DOD likely will be reviewing and analyzing SSPs and POAs both as part of the acquisition process and during contract performance, if an SSP or POA is vague or confusing, the DOD may ask the contractor questions or require additional information regarding the contractor's implementation of the NIST SP 800-171 controls or the DOD may reject the contractor's bid altogether. Likewise, contractors (and DOD officials) should anticipate bid protests implicating DFARS 252.204-7012, including challenges to the specific evaluation criteria an agency plans to use in evaluating the implementation of the NIST SP 800-171 controls and challenges to the government's evaluation of SSPs and POAs. Most importantly, contractors should expect the DOD to closely monitor their completion of the actions and meeting of the milestones in the POA. Failure to meet these milestones can amount to a breach of contract and be grounds for contract termination. Further, any inaccuracies or misrepresentations in an SSP or POA can be grounds for contract termination, and worse, form the basis of a fraud allegation.

Practical Implications for DOD Subcontractors

While the DOD requires its prime contractors to flow down DFARS 252.204-7012 to their supply chains, prime contractors adopt different approaches on when and how to flow down the clause.

For example, prime contractors use different criteria when deciding when to flow down DFARS 252.204-7012. Certain contractors heed the DOD's instruction for thoughtful and minimal flowdown and implement a targeted approach where they conduct an analysis of whether performance under a specific subcontract will require covered defense information or operationally critical support, and if so, will include DFARS 252.204-7012 in the subcontract. Many DOD prime contractors decline to take this approach, opting for a more conservative application of the rule, flowing down DFARS 252.204-7012 to all subcontractors, regardless of applicability.

The result is that subcontractors often are unable to decipher whether the DFARS rule actually applies to its performance and whether compliance is a condition of subcontract performance. Subcontractors who do not want to be bound by the clause are then forced to decide whether to turn down the government business or accept the clause and its requirements even though it may not touch covered defense information or provide operationally critical support. While some subcontractors will accept the inclusion of the clause in their subcontracts without a second thought, others will push back. This can lead to heated and challenging — and time-consuming — subcontract negotiations.

Further, prime contractors use different levels of diligence and oversight of their subcontractors when a decision is made to flow down DFARS 252.204-7012. Some prime contractors incorporate the clause into their subcontracts or purchase orders and take no further action. Other prime contractors, however, go one (or a few) steps further, requiring, among other things, that subcontractors:

- provide a certification regarding compliance with DFARS 252.204-7012 and the controls set forth in NIST SP 800-171;
- complete a detailed questionnaire regarding compliance with DFARS 252.204-7012 and the controls set forth in NIST SP 800-171;
- provide a copy of their SSP and POA;
- explain weaknesses in their information systems and issues encountered in implementation of the NIST SP 800-171 controls; and/or
- undergo an audit for compliance with the clause.

In response, subcontractors must decide whether to provide requested certifications, answer questions posed, or hand over SSPs and POAs, a decision that is not to be taken lightly since the consequences of refusing to provide such information can significantly impact the relationship between a prime contractor and subcontractor.

Last, DOD prime contractors manage their subcontractors differently, especially those that do not or cannot meet the requirements of DFARS 252.204-7012 or that refuse to provide requested information. A DOD prime contractor taking a hardline approach may be viewed as unreasonable, but so too could a subcontractor that refuses to provide requested information, causing a once-amicable relationship to sour not because of a legitimate threat, but because of a mere perceived one. Moreover, it can affect business opportunities because the prime contractor may not be able to bid on work without the subcontractor, and the subcontractor will lose the prime contractor's business.

What Should DOD Prime Contractors and Subcontractors Do to Avoid the Negative Consequences of These Requirements?

As the DOD continues its efforts to implement and enforce DFARS 252.204-7012, DOD contractors should take immediate and concrete actions to minimize the risks and consequences associated with the clause. Below are some practical tips.

- Analyze the applicability of the requirements and, where applicable, comply. If a contractor has not already done so, it should analyze whether it is contractually required to safeguard its information systems under DFARS 252.204-7012, and if so, whether and to what extent its information security controls meet those contained in NIST SP 800-171. This includes developing an SSP and POA that, together, describes the contractor's information systems, how those systems are protected and the concrete, discrete actions that the contractor will take to correct gaps or deficiencies in the systems' security, including how and when any unimplemented security requirements will be met. The SSP and POA must be clear, precise and accurate — the inclusion of false or misleading information in an SSP or POA could lead to an allegation of breach of contract or even fraud.

- Set yourself up for success. Contractors should make sure they have the resources and infrastructure to complete the actions and meet the deadlines set forth in the POA. This includes ensuring that appropriate stakeholders are engaged, assigned responsibility for meeting deadlines, provided needed resources and held accountable when deadlines are not met. Contractors must draft achievable POAs with an understanding that a failure to meet POA deadlines may amount to a breach of contract.

- Memorialize a policy on disclosing system security information. There is a significant uptick in requests by outside parties for contractor SSPs and POAs. In light of the highly proprietary and confidential information contained in SSPs and POAs, contractors should implement a policy that clearly memorializes when and to whom they will disclose them.

- Develop a clear procedure on subcontractor selection and management. DOD prime contractors should memorialize an approach to assess subcontractor compliance with DFARS 252.204-7012, including when it is appropriate to flow down the clause to its prospective and actual subcontractors. If a prime contractor anticipates providing covered defense information to its subcontractors, or if the subcontractor will be providing operationally critical support, the prime contractor should consider, at the opportunity development stage, whether the subcontractor's DFARS 252.204-7012 compliance program is adequate and can survive government scrutiny at the proposal stage, as well as a bid protest if the team is selected for an award. Prime contractors must be prepared to address the various issues raised by subcontractors, including refusal to provide an SSP or POA or refusal to submit a requested certification, or a subcontractor's attempt to negotiate DFARS 252.204-7012 out of their subcontracts.

- Establish a monitoring mechanism. Contractors should set up an infrastructure to monitor and adapt to changing cyber requirements — not just those promulgated by the DOD, but those issued by other agencies as well.

While the DOD information security requirements in DFARS 252.204-7012 likely will remain as clear as mud for the foreseeable future, contractors can begin to protect themselves from the unknown by taking action.

Jeniffer M. De Jesus Roberts is a partner and Katherine L. Veeder is a senior associate at Alston & Bird LLP.