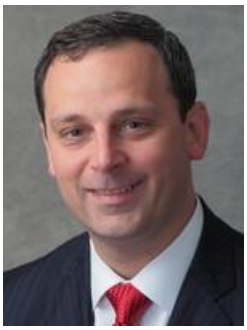
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Navigating Bid Protests Caused By DOD Cybersecurity Rules

By **Robert Metzger, Jeffery Chiow and Stephen Bacon, Rogers Joseph O'Donnell PC**

Law360, New York (April 18, 2017, 11:57 AM EDT) --


Robert Metzger


Jeffery Chiow


Stephen Bacon

By now contractors should be aware that U.S. Department of Defense solicitations must incorporate clauses that mandate the safeguarding of unclassified covered defense information from cyberthreats. Those provisions, specifically Defense Federal Acquisition Regulation Supplement 252.204-7008 and 252.204-7012, require contractors to represent and then provide "adequate security" for CDI that resides on their information technology systems by the end of 2017. At a minimum, contractors must implement the requirements specified by National Institute of Standards and Technology Special Publication 800-171.

Compliance with these new requirements will be challenging for many contractors, particularly small businesses. As with the introduction of any new regulation, ambiguities are bound to exist and result in compliance uncertainty. The significance of ambiguities may be magnified in a technical realm like cybersecurity where a complex web of industry standards and technical publications overlay the substantive contractual provisions that now govern.

The implementation challenges faced by contractors are likely to result in adverse agency evaluations of proposals, which will form the basis for bid protests. Perceived defects in an awardee's cybersecurity are also certain to be exploited by unsuccessful offerors seeking fodder for bid protests. While contractors bring their IT systems into compliance, they should be mindful of several key areas where bid protests may arise in connection with the DOD's new cybersecurity mandates.

Additional Security Requirements Beyond SP 800-171

The DOD has made available "Frequently Asked Questions" about the DFARS. The FAQs — a valuable resource for all contractors — emphasize that contracting officers should describe security requirements and assessments based on SP 800-171 and not on the more elaborate and demanding requirements of another NIST Publication, SP 800-53, that is intended for federal information systems and organizations rather than contractor information systems. However, recent experience indicates that some DOD components — and some civilian agencies — will include cyber compliance demands, for protection of CDI and other forms of controlled unclassified information on contractor systems, that are drawn from the "catalogue" of contract provisions and controls (such as

NIST SP 800-53) that were developed and intended for federal rather than contractor information systems. Faced with such demands, contractors could bring a "requirements" protest, to challenge the acquiring agency's selection of security requirements that go beyond SP 800-171.

That such a protest could have traction is illustrated by the U.S. Government Accountability Office's 2011 decision in Technosource.[1] There, protesters argued that a solicitation for cloud computing services included an unreasonable limitation on the countries where vendors could locate data centers and an unnecessary provision that restricted the government "community cloud" to government clients only. The GAO proceeded to consider whether the agency could justify these conditions. Regarding the limitation on the location of data centers, the GAO sustained the protest because the agency could not justify why the excluded countries were less secure. As for the restriction on co-tenants in the government "community cloud," the GAO denied the protest after considering applicable NIST guidance which demonstrated, as found by the GAO, that there were unique security vulnerabilities in a multi-tenant cloud environment.

There can be circumstances where protests properly challenge requirements that are excess to needs and unduly restrict competition, or which misapply federal requirements. However, the GAO should be restrained in its willingness to second-guess agency decisions on cyber requirements. This is not an area where the GAO examiners have relevant training. As concern DOD procurements, the cyber domain is one characterized by sensitive threat information, potential impacts with national security consequence, and technical complexity.

SP 800-171 Variance Requests

The -7008 DFARS solicitation clause includes a process by which offerors can seek approval to vary from any SP 800-171 requirements. (A similar process also is present in the -7012 contract compliance clause.) Before an award, an offeror can propose to vary from any of the security requirements of SP 800-171; it can submit to the DOD chief information officer a written explanation of why a particular security requirement is not applicable or how an alternative but equally effective measure is used instead. Such requests are to be "adjudicated" by a representative of the DOD CIO.

This process creates at least two potential protest issues. In the pre-award context, if an offeror's variance request is denied, and it faces exclusion from the competition, it could elect to protest the decision as unsupported. After award, an unsuccessful bidder might protest variances granted in order to displace an awardee from eligibility for award. In ruling on such protests, the GAO would be put in the delicate position of having to review security decisions previously made by the DOD CIO. The GAO has generally held that "where requirements relate to issues of human safety or national security, an agency has the discretion to define solicitation requirements to achieve not just reasonable results, but the highest possible reliability and effectiveness."[2] Cyberattacks on the DOD supply chain have significant national security consequences and thus the GAO should respect the DOD's expertise and treat variance decisions of the DOD CIO with great deference.

Cloud Service Providers and FedRAMP Compliance

The -7012 clause permits contractors to use a cloud service provider (CSP) to "store, process, or transmit" CDI if the CSP is compliant with the FedRAMP Moderate baseline or "equivalent" standards. Many contractors utilize cloud services. CDI received on a contract subject to the DFARS may be hosted on or processed in the cloud. Conceivably, a protest could arise if a contractor suffers a negative evaluation with respect to its treatment of CDI in the cloud. Disposition will be difficult because the

DFARS does not now state how a determination is to be made whether a CSP is "equivalent" or who is to make such a determination. This suggests that agency decisions on cloud suitability could be challenged on a "reasonableness" basis.

The GAO has already decided a protest concerning the issue of FedRAMP compliance, although it arose in the context of a federal information system requirement. In SRA International, the protester argued that the agency unreasonably found that it did not satisfy the solicitation's FedRAMP requirements.[3] The solicitation sought support for the agency's transition to a cloud-based email solution and required quoters to maintain an authority to operate at the time of quote. If quoters did not have an ATO, the solicitation included a provision that required quoters to provide: (a) documentation that confirmed that FedRAMP initiation had taken place; (b) a current ATO issued from another agency. The agency found that the protester failed to meet FedRAMP requirements because it did not provide evidence of an ATO from another agency under item (b). The protester argued that an ATO was not required because the FedRAMP requirements could have been met through satisfaction of items (a) or (b) and that it had satisfied item (a). The GAO agreed with the agency that the solicitation language required quoters to satisfy both items and denied the protest.

SRA International illustrates that solicitation language regarding cloud services and security requirements may be subject to high scrutiny. Agencies would be well counseled to describe carefully what they expect or require if offerors are allowed to use cloud for CDI. FedRAMP is an interagency federal process for accreditation of cloud services for federal agencies; if a procuring agency makes its own determination that a contractor has proposed use of cloud with security that is "equivalent" to FedRAMP, the agency should be very careful both to inform offerors what it expects and to document the basis of its determinations of "equivalency." At the same time, agencies should recognize that cloud service customers rarely have great leverage over the security or contracting practices of leading CSPs.

Adequacy of Promised DFARS Compliance

The DFARS clause, while imposed on all but commercial off-the-shelf suppliers to the DOD, does not require contractor compliance with NIST SP 800-171 as a mandatory evaluation factor in the source selection process. By submitting an offer, however, contractors "represent" that they will implement SP 800-171 "as soon as practical, but not later than December 31, 2017." The DFARS does not require contractors to submit any documentation with their proposal to demonstrate compliance — though a solicitation could include such a requirement.

Nevertheless, a disappointed offeror might challenge whether a procuring agency was justified in accepting an awardee's commitment to timely performance. In Discover Technologies, the protester argued that the awardee's proposal for website management support services should have been rejected because its web hosting vendor did not have authority to operate at the time of proposal submission and was therefore not in compliance with Federal Information Security Management Act requirements.[4] Because the solicitation imposed security requirements on the "contractor," as opposed to the bidding vendor, the GAO found that the relevant solicitation provisions were performance requirements that did not need to be satisfied before the award.

Similarly, the precise wording of the DFARS, at -7012(b), is that the "contractor" is to provide adequate security and, at -7012(b)(2)(ii)(A), the "contractor" is to implement SP 800-171 not later than Dec. 31, 2017. Satisfaction of prospective obligations under the DFARS should be treated as a matter of contract administration rather than a subject for protest. See 4 C.F.R. § 21.5(a). Where, in contrast, a solicitation calls for source selection assessment of a contractor's compliance with the DFARS and SP 800-171,

protests may arise from the agency's evaluation.

Cybersecurity as a Mandatory Evaluation Factor

In the DFARS FAQs, the DOD provides several examples of how it could consider compliance with the DFARS and SP 800-171 in the source selection process. One is to notify offerors that their approach to protecting CDI and providing "adequate security" in accordance with the DFARS will be evaluated on an "acceptable or unacceptable" basis. Another is to establish compliance with the -7012 DFARS clause as a "separate technical evaluation factor."

If a solicitation includes cybersecurity as a mandatory evaluation factor, the DOD may require offerors to submit a system security plan (SSP) for review, approval or evaluation. NIST released Revision 1 to SP 800-171 on Dec. 20, 2016. It adds a 110th security requirement that contractors prepare an SSP. In the SSP, the contractor must: "Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationship with or connections to other system."

Agency assessments of SSPs, and protester critiques of a competitor's SSP, generate scenarios where evaluations of SSPs could figure into protests. These are suggested by several GAO decisions involving claims that the agency unreasonably evaluated cybersecurity proposed by unsuccessful offerors or the eventual awardee.[5] In Atl. Sys. Group, Lintec and PricewaterhouseCoopers, the GAO either sustained or denied the protest on the basis that the proposal in question did not sufficiently address cybersecurity requirements. Procuring agencies should be careful when they request and in how they evaluate SSPs. The DOD's FAQs indicate that SSPs are not expected to promise or demonstrate either "instant" or "complete" compliance with SP 800-171 at the time of preparation. Rather, the FAQs recognize that a SSP may be used to describe how protections are implemented, address "individual, isolated or temporary deficiencies" and present "plans of action … to correct deficiencies and reduce or eliminate vulnerabilities."

The FAQs also indicate that a requiring activity may require an offeror to include elements of the SSP with its technical proposal (to be incorporated in the subsequent contract) and that the SSP may "inform a discussion of risk" between the contractor and the requiring activity or program office. Potential utilization of the SSP for these purposes does raise the possibility of "disparate treatment" (real or alleged) and of selection decisions that lack supporting documentation or otherwise fail to possess a reasonable basis. Considering the likely importance of cybersecurity compliance in future procurements — and evaluations — procuring authorities ought to be very deliberate and specific in what they include in requests for proposals as to SSP-related requirements and in how they evaluate and act upon SSPs when required for selection and award. Otherwise, the well-intended and important role of SSPs in the achievement of security could further fuel protests.

Conclusion

Federal information, when shared with contractors, must be protected. Under the "Network Penetration" DFARS, defense suppliers must provide "adequate security" and implement the 110 controls of SP 800-171. Civilian agencies will follow suit for protection of all the many forms of "controlled unclassified information." These are important, but difficult obligations. They should not become "fodder" for the protest mill. But compliance with cyber contract requirements will come to figure importantly in eligibility and selection decisions. Even though agency decisions on cyber adequacy should receive great deference, they will not be immune from challenge in the protest venues. The

traditional doctrines for protest challenge will apply. Agencies have the key role. They must be discriminating and informative in the application of cyber requirements and careful in their evaluation of cyber submissions such as SSPs. They must document both what they expect and how they evaluate these submissions. At the same time, contractors facing cyber demands in solicitations and in new contracts also should be careful to determine that the requirements are appropriate and achievable, do not limit competition improperly, that the cyber duties are fairly applied, and that evaluations of cyber plans or accomplishments are reasonable and documented.

Robert Metzger is a shareholder at Rogers Joseph O'Donnell PC and head of the firm's Washington, D.C., office. Jeffery Chiow is a shareholder in the firm's Washington office. Stephen Bacon is an associate in the firm's Washington office.

[1] Technosource Info. Sys., LLC, et al., B-405296, B-405296.2, Oct. 17, 2011, 2011 CPD ¶ 220.

[2] Coulson Aviation (USA), Inc., B-411525, Aug. 14, 2015, 2015 CPD ¶ 272 at 15 (citing Womack Mach. Supply Co., B-407990, May 3, 2013, 2013 CPD ¶ 117 at 3).

[3] SRA Int'l, Inc., B-409939, Sept. 2, 2014, 2014 CPD ¶ 264.

[4] Discover Technologies LLC, B-412773, B-412773.2, May 27, 2016, 2016 CPD ¶ 142.

[5] See, e.g., Atlantic Sys. Group, Inc., B-413901, B-413901.2, Jan. 9, 2017, 2017 U.S. Comp. Gen. LEXIS 26 at *9-10 (upholding the agency's determination that the protester's proposal lacked sufficient details regarding the implementation and assessment of security controls because the protester "should have been aware that a detailed explanation of what it intended to do to accomplish the work was required."); LINTECH, LLC, B-409089, B-409089.2, Jan. 22, 2014, 2014 CPD ¶ 38 at 4 (denying the protester's challenge to the agency's evaluation because the "proposal does not at all address compliance with security requirements of FISMA, NIST, and VA Directive 6500."); Pricewaterhouse Coopers LLP, B-409537, B-409537.2, June 4, 2014, 2014 CPD ¶ 255 at 6 (sustaining a protest where the agency's "best value" judgement failed to appropriately consider that the awardee's technically inferior proposal which did not include sufficient details regarding its "proposed methods and tools for conducting network vulnerability assessments and penetration tests.").
