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

What DOD's Use Of Cyber Scores May Mean For Contractors

By **Robert Metzger, Deborah Rodin and Eleanor Ross**
(November 2, 2020, 3:59 PM EST)

Robert Metzger

Deborah Rodin

Eleanor Ross

On Sept. 29, the U.S. Department of Defense published the interim rule implementing the Cybersecurity Maturity Model Certification, or CMMC, program. The interim rule will require 20,000-plus companies to report a self-assessment of their cyber compliance to the DOD.

New contract clauses that mandate this reporting will appear in solicitations and other contract actions after Nov. 30. What use will the DOD make of the soon-to-be-required cyber self-assessment score?

Although the interim rule does not say, this article suggests how the DOD may use the assessment as part of its responsibility determination or as technical evaluation criteria. Because future business opportunity may depend upon the self-assessment score, this article offers guidance for contractors to consider now.

It is not new that the DOD requires compliance with the 110 cybersecurity requirements set forth in the National Institute of Standards and Technology Special Publication 800-171 to provide adequate security measures, per Defense Federal Acquisition Regulation Supplement clause 252.204-7012.

What is new is that the DOD will now require contractors to post on DOD's Supplier Performance Risk System, or SPRS, a score that reflects the contractor's accomplishment of the NIST cybersecurity requirements.

The New DOD Assessment

The DOD's interim rule is implemented by DFARS clauses 252.204-7019 and 7020, which require use of a standard assessment and scoring methodology.[1] A score of 110 is realized if all requirements are fully satisfied. Points are deducted for NIST SP 800-171 controls not implemented.

The assessment methodology is not designed to credit partial implementation.[2] Contractors may actually receive a score below zero because the scoring system assigns different weights to individual security requirements.

Until now, contractors could be compliant with the DFARS 7012 clause even if they did not meet all 110 requirements, as long as they had a plan of action and milestones to correct or mitigate deficiencies in their system security plans.[3] Now that contractors must report their self-assessment to the DOD, many may submit scores lower than 110, and possibly significantly lower.

The interim rule currently requires contracting officers to ensure only that contractors have a current summary-level assessment score on record in the SPRS prior to award. The rule does not set any numeric threshold out of the maximum score of 110 or establish what might be considered a score so low as to be unacceptable.[4]

Nor does the rule state whether the score will be used in the source selection process. But the DOD is unlikely to ignore the import of low scores on all procurements. We expect that the DOD will consider the posted SPRS score in determining a contractor's responsibility or in evaluation criteria.

The DOD Assessment as a Responsibility Criteria

All prospective contractors must be found to be responsible to receive award, pursuant to Federal Acquisition Regulation 9.103. The DOD's cyber-assessment score may figure into a contracting officer's responsibility determination, either as a general consideration or as a special standard.

Including the NIST SP 800-171 cyber score in a responsibility determination could have far-reaching implications.

1. General Standards of Responsibility

Separate from the cyber interim rule, the DOD recently proposed a rule that requires contracting officers to use information from the SPRS in determining whether a prospective contractor is responsible. This rule provides a basis for the DOD to use NIST SP 800-171 assessment scores reported in the SPRS in determining contractor responsibility.

Responsibility is based on FAR 9.104-1, which includes several criteria such as resources, capability to perform and record of ethical conduct.[5] Contractors must be "otherwise qualified and eligible," which encompasses collateral requirements, or other provisions of law that could make a contractor ineligible.[6]

While these collateral requirements typically promote the government's socioeconomic goals, the new cyber score could be considered a collateral requirement.

In the proposed SPRS rule, the DOD clarifies that a factor to use in determining contractor responsibility is the supplier risk assessment, which "highlights for the contracting officer the probability that an award made to a supplier may subject the procurement to the risk of unsuccessful performance or to supply chain risk."[7]

The proposed rule would require evaluation of SPRS data from multiple sources, including data that informs supply chain risk.[8] The NIST SP 800-171 assessment is not currently included in the SPRS data considered in determining contractor responsibility.

However, because the DOD has made improved contractor cybersecurity a very high priority, companies should appreciate that contracting officers soon will have cyber scores posted to SPRS and may consider

those scores in making the supplier risk assessment.[9]

The NIST SP 800-171 assessment score provides an additional data point to assess supplier risk. Contracting officers may conclude that very low cyber scores denote excess risk.

Thus, the cyber assessment score may figure into a contracting officer's general responsibility determination. Case law shows that, "[b]ecause responsibility decisions are largely a matter of judgment, contracting officers are generally given wide discretion to make this decision."[10]

It is not yet known when a contracting officer will consider any assessment score or whether a low score could lead to a contractor being found nonresponsible. Unless the DOD further defines how it will use the scores, companies with low scores will face uncertainty, and contracting officers could take inconsistent actions on different procurements, contributing to frustration and possible legal challenges.

The DOD should clarify whether and how the cyber-assessment score entered in the SPRS will be used in a responsibility determination. It strains credulity that the DOD would be content to know only that a score — any score — was posted, irrespective of whether it is a perfect 110 or some much lower number.

If the scores are in the SPRS for the purpose of determining contractor responsibility, the supplier community needs to know the plan.

2. Special Standards of Responsibility

Contracting officers might also identify a threshold score on the DOD cyber assessment as a special standard, or definitive criteria, for contractor responsibility. These are "specific and objective standards established by an agency for use in a particular procurement for the measurement of a bidder's ability to perform the contract."[11]

Using special standards, the government can prescribe in more detail the minimum standards or qualifications necessary for contract performance. To ensure fairness, special standards must be expressly identified as such in the solicitation, must apply to all bidders, and cannot be waived by the contracting officer.[12]

Pursuant to FAR 9.104-2, contracting officers have broad discretion to determine when special standards of responsibility are necessary for a particular acquisition or class of acquisitions, and they are often used when unusual expertise, special facilities or specific experience is necessary to meet the agency's needs.

Case law supports a deferential view of special standards, so long as they are necessary to meet the agency's minimum needs.[13]

As a result, contracting officers may be able to set a certain level of compliance with the NIST SP 800-171 requirements as necessary for the agency's needs. Identifying the minimum required score as a special standard of responsibility in the solicitation would provide contractors with reasonable advance notice. The score might be required at the time of award.

The DOD Assessment as Evaluation Criteria

The DOD also could use the NIST SP 800-171 assessment score as part of its evaluation criteria — either as gate criteria or as Section M evaluation criteria.

If used as gate criteria, the cyber assessment would be the first step in the agency's evaluation of the offeror's ability to meet the contract requirements. An agency may use gate criteria to establish certain minimum criteria for bidders before they can compete for a contract.[14]

For illustration, the DOD might require offerors to have a posted score of 90 or above, prior to proposal submission; otherwise they would be eliminated from the competition.

Agencies may consider NIST SP 800-171 assessment scores in the evaluations of offerors' proposals. As part of the award decision, the agency would determine whether the offeror meets the minimum score, or it could provide favorable evaluation credit for higher scores.

Alternatively, an agency could include a minimum NIST SP 800-171 assessment score in a performance work statement or at some other specified time during performance. Therefore, an agency could allow offerors to demonstrate they have the specified minimum score at award or even within some amount of time, e.g., 30 days, after contract award.

The method that the agency chooses to evaluate the new NIST SP 800-171 assessment will have an impact on when an offeror could challenge the requirement or the evaluation. If an offeror objects to the DOD requiring a minimum score as part of the solicitation, a preaward protest challenge would be required. Unsuccessful offerors may protest post-award to challenge a score claimed — and posted on the SPRS — by successful bidders.

Recommendations for Contractors

In just a few weeks, beginning Nov. 30, contractors will begin to receive solicitations and enter into contracts requiring the NIST SP 800-171 self-assessment and the SPRS posting requirement. Here are a few suggestions for contractors to consider as they start responding to the new requirements.

1. If a solicitation has DFARS clauses 252.204-7019 and 7020, but no information about how the contracting officer will use the assessment score, contractors should ask the contracting officer whether and how the assessment will be used.

2. Where a solicitation references the NIST SP 800-171 score either as special standards for responsibility, or as gate or evaluation criteria, any challenges to the use of such criteria must be raised prior to the date proposals are due.

3. This interim rule could change based on comments received by the DOD by Nov. 30. Companies can submit comments with opinions on how to clarify use of the NIST SP 800-171 assessments.

4. Contractors should act promptly to conduct self-assessments and act to achieve a perfect compliance score of 110. Given the uncertainty about how lower scores will be considered in the source selection process, achieving full compliance may be an excellent investment.

Robert S. Metzger is a shareholder, and Deborah Norris Rodin and Eleanor Ross are associates, at Rogers Joseph O'Donnell PC.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Basic assessments will be completed by the contractor itself using the specified DOD methodology. For contracts involving more sensitive information, the Defense Contract Management Agency may perform on-site medium- and high-level assessments.

[2] The DOD assessment is done using the DCMA NIST SP 800–171 DOD assessment methodology, available https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html. The level of assessment reflects the depth of the assessment performed and the associated level of confidence the DOD has in the assessment.

[3] To document their compliance, system security plans describe how contractors meet security requirements; plans of action and milestones describe how they intend to satisfy any unmet requirements.

[4] In recently updated Cybersecurity FAQs, the DOD indicated that it did not plan to impose a pass/fail scoring threshold for the NIST SP 800-171 assessment to comply with DFARS clause 252.204-7012. However, the "decision to accept the risk should remain with the Requiring Activity." This seems to enable the DOD components to make their own determination on whether to use a scoring threshold. DOD, Cyber DFARS FAQs rev 3 (July 30, 2020) at Q126, available at https://dodprocurementtoolbox.com/faqs/cybersecurity/cybersecurity-faqs-0.

[5] FAR 9.104-1.

[6] See FAR 9.104-1(g).

[7] Proposed Rule, "DFARS: Use of Supplier Performance Risk System (SPRS) Assessments," 85 Fed. Reg. 53748-49 (Aug. 31, 2020).

[8] See SPRS Evaluation Criteria (July 2019), at 6-7 (discussing sources for and the method of calculating supplier risk scores).

[9] See SPRS User's Guide version 3.2.11 (Sept. 2020), at 7-8.

[10] John C. Grimberg Co. v. U.S., 185 F.3d 1297, 1303 (Fed. Cir. 1999).

[11] Chas. H. Tompkins Co. v. U.S., 43 Fed. Cl. 716, 720 (1999).

[12] See FAR 9.104-2; John C. Grimberg Co., 185 F.3d at 1301.

[13] See, e.g., Navajo Nation Oil & Gas Co., B-261329, Sept. 14, 1995, 95-2 CPD ¶ 133.

[14] See, e.g., Oracle Am. Inc., v. U.S., 975 F.3d 1279 (Fed. Cir. 2020) (upholding elimination of bidder for failure to meet gate criteria); ATSC Aviation, LLC v. U.S., 141 Fed. Cl. 670 (2019) (upholding gate criteria requiring an AS 9100 quality assurance certification).