Published on *The National Law Review* https://natlawreview.com

New Cybersecurity Assessment Requirement for Department of Defense Contractors Effective November 30, 2020

Article By:

Erin L. Toomey

Frank S. Murray

Jennifer L. Urban

Samuel D. Goldstick

As of November 30, 2020, certain U.S. Department of Defense ("DoD") prime contractors and subcontractors will need to complete a cybersecurity self-assessment prior to receiving new DoD contracts and prior to the exercise of new options under existing DoD contracts. Additionally, DoD contractors will need to ensure that any subcontractors that receive Controlled Unclassified Information ("CUI") have also completed the cybersecurity self-assessment.

Existing Cybersecurity Requirements for DoD Contractors

DoD currently requires that all contracts, except for contracts for commercially available off-the-shelf ("COTS") items, contain Defense Federal Acquisition Regulation Supplement ("DFARS") clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, which requires that the contractor implement the 110 security controls set forth in National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171 on any information system that processes, stores, or transmits CUI. A contractor that has not fully implemented all 110 of the NIST SP 800-171 security controls is permitted to submit a so-called "system security plan" or "SSP" that describes the system architecture and current level of implementation of each of the required controls. For any controls not yet fully implemented, contractors are required to submit a Plan of Action and Milestones or "POAM" that identifies the steps to be taken to implement those controls and the anticipated timeframe for completion of those steps.

DoD has historically permitted contractors to self-attess to their compliance with the NIST SP 800-171 controls, and the SSP and POAM construct has permitted contractors to win DoD contracts

and subcontracts involving CUI without having fully implemented all of the NIST SP 800-171 controls required by the DFARS cybersecurity clause. DoD has become concerned that the current cybersecurity compliance approach does not ensure sufficient protection of CUI in contractor systems and fails to provide DoD with sufficient insight into the cybersecurity posture of companies within the Defense Industrial Base.

New Requirement for NIST SP 800-171 Assessments

On September 29, 2020, DoD issued a new interim rule designed to address these perceived deficiencies in the current cybersecurity framework by providing DoD with objective cybersecurity "scores"—and, ultimately, certification levels—for defense contractors and subcontractors. Importantly, the interim rule created a new NIST SP 800-171 Assessment requirement that will apply to all DoD contracts or orders awarded on or after November 30, 2020 that exceed the micro-purchase threshold (currently $10,000 for most types of procurements), except for contracts or orders exclusively for COTS items. The new NIST SP 800-171 Assessment requirement will be imposed through the inclusion in new DoD solicitations of DFARS clause 252.204-7019, *Notice of NIST SP 800-171 DoD Assessment Requirements*. This new DFARS clause will impose a requirement for offerors to have on file with DoD a NIST SP 800-171 Assessment performed within three years of the contract award, in order for the offeror to be considered for award of the contract (or issuance of a task or delivery order) under the solicitation. A NIST SP 800-171 Assessment is to be completed on each contractor information system that would be handling CUI under the contract or order.

Contractors with options on existing contracts that will be exercised on or after November 30, 2020 will also need to ensure that a NIST SP 800-171 Assessment has been performed and submitted to DoD within three years of the option exercise date.

The required NIST SP 800-171 Assessment can be performed by DoD itself, though DoD has limited bandwidth to audit contractor information systems and will therefore be able to conduct its own assessment on only a relatively small number of defense contractors and subcontractors within any three-year period. The remaining contractors and subcontractors that will be handling CUI on their information systems are required to perform and document a *self*-assessment.

Three Assessment Levels

There are three possible "assessment levels" for a NIST SP 800-171 Assessment, reflecting the varying levels of DoD involvement and the corresponding degree of confidence DoD assigns the numerical point-score reported from the assessment. A contractor self-assessment is referred to as a "Basic Assessment." The contractor is to perform its self-assessment based on a review of the SSP(s) for the contractor's information system(s), following the guidance set forth in NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information" (guidance that is recounted in the assessment methodology posted by DoD at the hyperlink below). Because the Basic Assessment is performed without DoD involvement, DoD assigns a "Low" confidence level to the contractor's self-generated point-score.

A "Medium Assessment" is a NIST SP 800-171 Assessment of the contractor's information systems conducted by DoD personnel, but without direct DoD inspection or observation of the contractor's information systems. A Medium Assessment consists of DoD review of the contractor's self-assessment, "a thorough document review," and discussions between DoD and the contractor to obtain additional information or clarification, as needed. Because DoD will be obtaining at least some documentary support for the contractor's self-generated score and modifying the score as deemed

appropriate, DoD assigns a “Medium” confidence level to the score resulting from a Medium Assessment.

The most in-depth assessment of a contractor’s implementation of NIST SP 800-171 is referred to as a “High Assessment.” A High Assessment builds upon the steps involved in a Medium Assessment by adding verification, examination, and demonstration of the contractor’s SSP to validate that the NIST SP 800-171 controls have been implemented as described in the plan. In other words, a High Assessment includes DoD inspection of the contractor’s information system and security controls to validate the information reported in the SSP, which results in DoD assigning a “High” confidence to the point-score obtained through this type of assessment.

Assessment Methodology and Scoring

DoD has posted guidance regarding NIST SP 800-171 Assessments here. The current guidance regarding the methodology and scoring for NIST SP 800-171 Assessments, updated on June 24, 2020, can be found here.

The NIST SP 800-171 Assessment examines which of the 110 NIST SP 800-171 security controls the contractor has implemented and uses a weighted scoring system to assess the level of risk posed by the contractor’s failure to implement all of the required controls. If a contractor has implemented all of the security controls, it would receive a “perfect score” of 110 points. Points are deducted for security controls that have not been implemented, with a weighted scoring system that deducts more points for controls deemed to have a greater impact on the overall security risk posed by the contractor’s information system.

Reporting the Assessment

The results of NIST SP 800-171 Assessments are to be reported in the Supplier Performance Risk System (“SPRS”), an internal system accessible to DoD contracting personnel. DoD itself is responsible for reporting the results of Medium or High Assessments, given DoD’s involvement in the validation of those assessment scores. However, contractors (and subcontractors) themselves are responsible for reporting the results of a self-performed Basic Assessment. New DFARS clause 252.204-7019 spells out the procedures contractors should follow in reporting the results of their Basic Assessments.

Flow-Down and Subcontractor Compliance

Contractors are also required to flow down new contract clause DFARS 252.204-7020, *NIST SP 800-171 DOD Assessment Requirements* in all subcontracts or orders except for those exclusively for COTS items. This clause prohibits the contractor from awarding a subcontract (or issuing a purchase order) that will involve access to CUI to any subcontractor that has not completed a NIST SP 800-171 Assessment within the last three years. If a subcontractor does not have a “current” (within the past three years) NIST SP 800-171 Assessment score posted in SPRS, the subcontractor needs to perform and submit to DoD a Basic Assessment via encrypted e-mail.

The new contract clause, however, does not address how a contractor is expected to verify that prospective subcontractors have completed a current NIST SP 800-171 Assessment since contractors only have access in SPRS to check *their own* NIST SP 800-171 Assessment scores; unlike DoD personnel, contractors do not have access to SPRS records of other entities. As a result,

contractors will presumably find it necessary to develop new supplier or subcontractor certifications addressing the submission of NIST SP 800-171 Assessment scores to DoD.

Open Issues in the Interim Rule

Some key considerations are left unaddressed by the interim rule. For example, the interim rule indicates that DoD will treat NIST SP 800-171 Assessment results as CUI and exempt such results from disclosure under the Freedom of Information Act as "trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential." Does that mean that a prime contractor cannot require a subcontractor to disclose its most recent NIST SP 800-171 Assessment scores, as part of the certification used by the prime contractor to validate that a subcontractor has a "current" NIST SP 800-171 Assessment posted in SPRS?

The new rule also does not make clear whether or how DoD intends to use the NIST SP 800-171 Assessment scores posted in SPRS as part of the procurement process. For example:

- Will DoD allow its components to use the summary-level point scores as part of the qualitative evaluation of offerors' proposals in procurements involving CUI?
- Will the scores become part of the evaluation of an offeror's "past performance" or performance risk? If so, how would DoD compensate for the differing confidence levels of a score obtained under a DoD-performed Medium or High Assessment, as compared to a contractor's self-generated score under a Basic Assessment?
- Given that DoD will have access to subcontractor assessment point-scores in SPRS, while a prime contractor would not, will contracting officers hold a low-scoring subcontractor's increased cyber-risk against the prime contractor in a competitive procurement?
- Will DoD contracting officers use the scores as part of their determinations of a prospective awardee's present responsibility? If so, how low a score would be deemed to jeopardize a contractor's eligibility for award of a contract involving CUI?
- Will DoD contracting officers use these NIST SP 800-171 Assessment scores posted in SPRS as the basis for disapproving the contractor's use of particular subcontractors on contracts that call for Government approval of subcontracts?
- Under what circumstances, if any, can a contractor use a self-performed Basic Assessment to displace an earlier DoD-performed Medium or High Assessment?

Contractors seeking clarification of these or other issues raised by the new interim rule, or seeking changes to the rules themselves, should consider filing comments to DoD on the interim rule by the comment due date of November 30, 2020.

What Do Contractors Need to Do Now?

The new NIST SP 800-171 Assessment requirements will go into effect on November 30, 2020. DoD prime contractors and subcontractors (other than COTS providers) should take the following steps to comply with the new self-assessment requirements:

- Contractors should check the SPRS to determine whether it contains a NIST SP 800-171 Assessment score for them, and the date on which the assessment was performed. While access to most of SPRS' functionality is limited to DoD personnel, authorized representatives of a contractor are permitted to access SPRS to view the contractor's own summary-level NIST SP 800-171 Assessment score. Guidance for contractors on how to obtain access to SPRS to review their own NIST SP 800-171 summary-level scores can be found in the SPRS Software User's Guide for Awardees/Contractors, available here.

- If a contractor does not have a NIST SP 800-171 Assessment score posted on SPRS, the contractor should perform a Basic Assessment of its own implementation of the NIST SP 800-171 security controls prior to November 30, 2020 so that it can report the score by that date. New DFARS clause 252.204-7019 specifies the information contractors are required to report to SPRS and the e-mail address to which they are to report that information: webptsmh@navy.mil. Given the sensitivity of the information, contractors are instructed to report their Basic Assessment information via encrypted e-mail.

- The Basic Assessment report should address, for each SSP supporting the performance of a DoD contract: (i) all Commercial and Government Entity ("CAGE") codes associated with the information system(s) addressed by the SSP and a brief description of the SSP architecture, if more than one plan exists; (ii) the date the self-assessment was completed; (iii) the summary-level score achieved (*i.e.*, the total point-score after making any deductions necessary from the "perfect" score of 110); and (iv) the date that all requirements are expected to be implemented (*i.e.*, the date by which the contractor expects to be able to achieve a perfect score of 110).

- Develop internal controls regarding how to flow down NIST SP 800-171 Assessment requirements to subcontractors and suppliers, including: (i) determining when NIST SP 800-171 compliance is required for subcontractors and suppliers (to the extent the company has not done that already); and (ii) develop a new subcontractor certification or other method of ensuring, prior to award of a new subcontract or purchase order, that subcontractors and suppliers that will have access to CUI under a DoD contract have a "current" NIST SP 800-171 Assessment posted on SPRS; and

- Have discussions with teaming partners, subcontractors, and suppliers to ensure that all parties that will be required to perform a self-assessment will be able to do so prior to the award of new contracts.

The NIST SP 800-171 Assessment requirement appears to be an interim measure before DoD fully implements the Cybersecurity Maturity Model Certification ("CMMC") framework that eventually will apply to all DoD contractors, subcontractors, and suppliers and will involve cybersecurity assessments performed by third party assessment organizations. Although the CMMC requirements could be included in DoD contracts starting as soon as November 30, 2020, the CMMC framework will be rolled out slowly and will not apply to all DoD contracts until 2025. In the interim, DoD contractors will have to comply with the new NIST SP 800-171 Assessment requirements effective November 30, 2020.

National Law Review, Volume X, Number 294

Source URL:https://natlawreview.com/article/new-cybersecurity-assessment-requirement-department-defense-contractors-effective