New interim rule continues DoD push to increase the security and resilience of the Defense Industrial Base sector

Beginning November 30, 2020, defense contractors (except those only providing commercially available off-the-shelf items [COTS]) will be required to file an assessment of their NIST SP 800-171 compliance with the Department of Defense (DoD) to be considered for award of a contract.

A current assessment report (not more than three years old) will need to be on file with the DoD before new contracts will be awarded. The DoD first introduced this new requirement on September 29, 2020, with the issuance of a new interim rule, which amends DFARS Subpart 204.73 and adds DFARS Subpart 204.75.

In addition to the NIST SP 800-171 filing with the DoD, the interim rule formally establishes the requirement for Cybersecurity Maturity Model Certification (CMMC) in order to verify the processes and practices expected of a given cybersecurity maturity level.

New reporting requirement NIST SP 800-171 assessment

The requirement for DoD contractors and subcontractors to safeguard covered defense information isn't new. It was originally required per DFARS 252.204-7012 no later than December 31, 2017, and applies to covered contractor information systems that are not part of an IT service or system operated on behalf of the Government.

The DoD recognized inconsistencies in the completeness and accuracy of cybersecurity control reporting and introduced the new DFARS provision 252.204-7019, which now requires all Basic level self-assessments to be reported directly to the DoD via the Supplier Performance Risk System (SPRS). Additionally, the DoD has decided that Government representatives will be completing the assessment for Medium- and High-risk contractors.

When completing a self-assessment, contractors will be responsible for entering six fields into SPRS:

1. System Security Plan name
2. CAGE code associated with the plan
3. Brief description of the plan architecture
4. Date of the assessment
5. Total score
6. The date a score of 110 will be achieved

In the event that the DoD requires a higher-level assessment than the Basic level, the contractor is required to provide the government with access to facilities, personnel and systems so they can conduct the higher-level assessment.

The assessment uses a weighted scoring methodology to indicate the net effect of requirements not yet implemented by the contractor. While the controls themselves are not prioritized, certain controls have greater impact and are worth more points. Effective November 30, 2020, contracting officers at the DoD will be directed to verify the contractor's assessment is current (not older than three years) and on-record in SPRS prior to awarding the contract. Because the record in SPRS reflects the total achieved score, it's reasonable to conclude that contracting officers will be able to compare assessment results for competing contractors when determining supplier quality.

CMMC requirements formalized

The objective of CMMC hasn't changed since the DoD originally announced the program. The interim rule establishes the DFARS Subpart 204.75, which specifies the policies and procedures for awarding a contract that includes a requirement for CMMC certification. Also new is DFARS clause 252.204-7021, which, except for the acquisition of completely COTS items, requires a contractor to maintain the "requisite CMMC level for the duration of the contract" and establishes the flow down requirement "to ensure that its subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments."

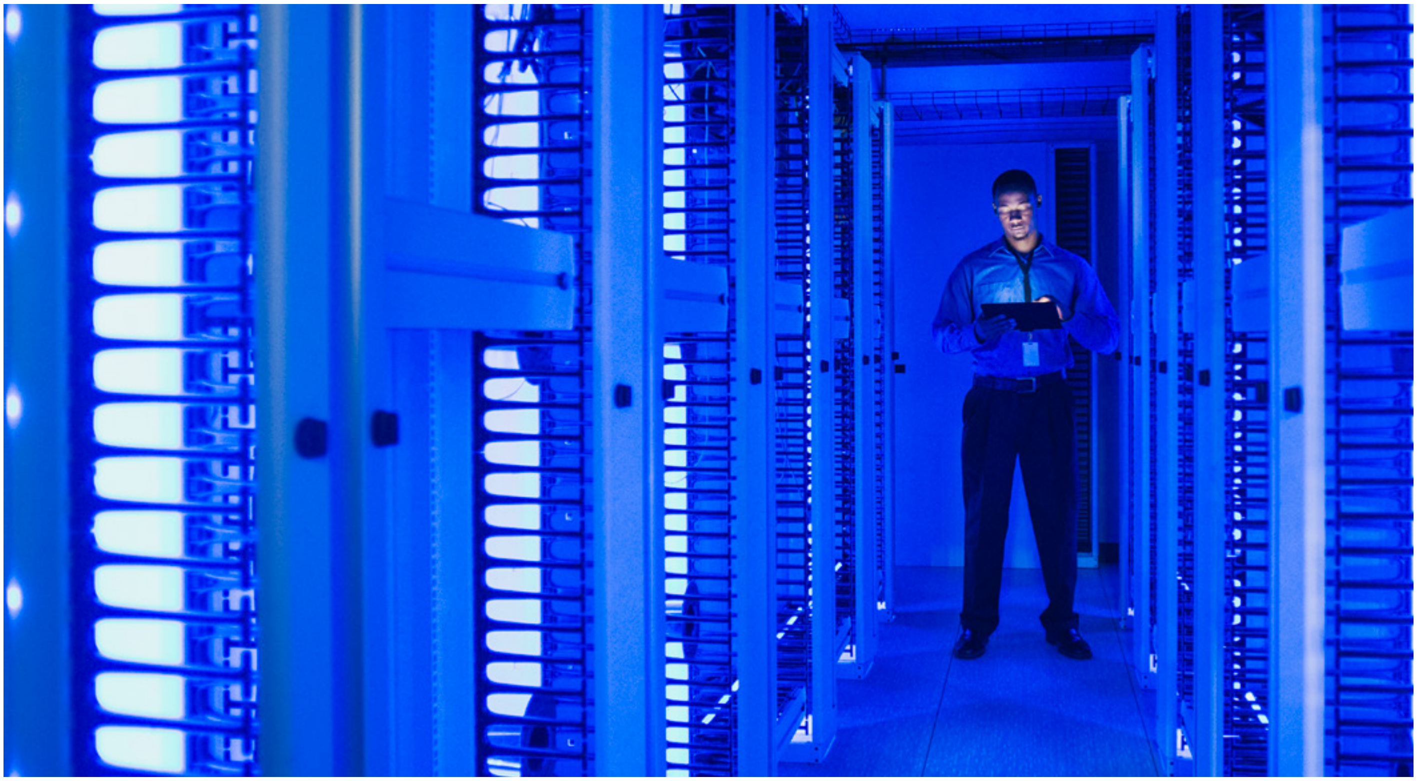
The CMMC model includes cybersecurity practices organizations are required to implement in order to safeguard information assets, as well as the processes to ensure consistent maturity within the organization. The model contains five levels of maturity that progress from performing basic cyber hygiene at level 1 to optimizing advanced cybersecurity at level 5.

The DoD expects most contracts to require level 3 certification — managed, good cyber hygiene — and high sensitivity contracts will require level 4 or level 5 certification. In the interim rule, the DoD reiterates that contractors should have already implemented all 110 controls from NIST SP 800-171 and focuses on the incremental practices and processes contractors are required to implement.

CMMC Level	Description
1	Consists of the 15 basic safeguarding requirements from FAR clause 52.204-21
2	Consists of 65 security requirements from NIST SP 800-171 implemented via DFARS clause 252.204-7012, 7 CMMC practices and 2 CMMC processes. Intended as an optional intermediary step for contractors as part of their progression to Level 3.
3	Consists of all 110 security requirements from NIST SP 800-171, 20 CMMC practices, and 3 CMMC processes.
4	Consists of all 110 security requirements from NIST SP 800-171, 46 CMMC practices, and 4 CMMC processes.
5	Consists of all 110 security requirements from NIST SP 800-171, 61 CMMC practices, and 5 CMMC processes.

What you need to know now

- Create account in Supplier Performance Risk System, which requires registration through Procurement Integrated Enterprise Environment.
- Enter your NIST SP 800-171 assessment details prior to pursuing your next contract. While the DoD expects these assessments to already be completed, we anticipate that many subcontractor organizations will need to conduct an initial assessment.



- Consider remediating control gaps and increasing your score before filing your assessment in SPRS. Each control not implemented deducts one point from the maximum achievable score of 110. Given that contracting officers can view scores across all offerors, a lower score could be interpreted as reduced supplier quality.
- Begin planning for CMMC, which has additional control requirements above and beyond NIST SP 800-171 and involves increased levels of documentation and process maturity. The jump from a level 1 to a level 3 can be a big lift and make take 12-24 months to fully implement. With certification requirements being phased in over the next five years, it makes sense to start now and build realistic budgets to mature your cybersecurity management program.

Wipfli can help you assess the current state of your cybersecurity management program and identify any necessary improvements that you'll need to make in order to comply. Contact us to learn more.

Related content

DoD adds critical verification component to defense contractor cybersecurity requirements

Webinar: What you need to know to comply with DoD cybersecurity certification requirements

WIPFLI