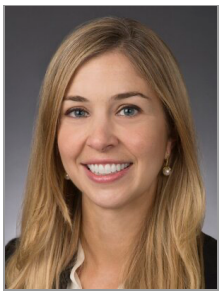
LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

4 Ways To Prepare For DOD Cyber Certification Rule

By **Townsend Bourne and Lillia Damalouji** (September 30, 2024, 5:03 PM EDT)



Townsend Bourne

Lillia Damalouji

The U.S. Department of Defense recently **released** a highly anticipated proposed rule to implement the Cybersecurity Maturity Model Certification, or CMMC, program.[1]

The proposed Defense Federal Acquisition Regulation Supplement rule, which was published in the Federal Register on Aug. 15, mirrors changes in a **December 2023** proposed rule and, once finalized, will be rolled out in phases over a three-year period.

The recently proposed rule significantly expands the text of the new DFARS CMMC clause, DFARS 252.204-7021, initially published by the DOD in January 2023, to require that contractors:

- Have a current CMMC certificate or self-assessment at the requisite CMMC level, or higher;
- Maintain the required CMMC level for the duration of the contract for all applicable information systems;
- Only store, process or transmit data in appropriate information systems;
- Notify the contracting officer within 72 hours of any lapses in information security or changes in the status of CMMC certificate or self-assessment levels;
- Complete and maintain annually, or when changes occur, an affirmation of continuous compliance with the security requirements; and
- Ensure all subcontractors and suppliers complete and maintain annually, or when changes occur, an affirmation of continuous compliance with the security requirements.

In addition, the proposed clause includes a new section on reporting (1) the unique identifiers for each information system included in the DOD's Supplier Performance Risk System; (2) the results of contractor self-assessments in SPRS; and (3) any changes to the list of unique identifiers.

Given the federal government's increased scrutiny of contractor compliance with cybersecurity requirements under the U.S. Department of Justice's Civil Cyber-Fraud Initiative. It is critical that contractors begin preparing now for the upcoming implementation of CMMC requirements.

On Aug. 22, the DOJ announced that it had **joined a whistleblower suit** and filed a complaint-in-intervention against the Georgia Institute of Technology and the Georgia Tech Research Corp. in the U.S. District Court for the Northern District of Georgia,[2] raising claims under the False Claims Act for failure to meet cybersecurity

requirements in connection with DOD contracts.[3]

As DOD contractors and subcontractors prepare for CMMC to take effect in 2025, they should take key actions in critical areas the government is likely to focus on in light of the Georgia Tech civil cyber fraud case.

1. Determine the CMMC levels that are likely to apply to future contracts.

CMMC requirements will apply to all contractor systems that store, process or transmit controlled unclassified information, or CUI, or federal contract information, or FCI, in performance of the contract, with certain limited exceptions.

While CUI has been a focus for contractors, requirements for FCI will become more important as companies must provide attestations and confirm self-assessments for FCI's 15 basic security controls.

When a CMMC level is included in a solicitation or contract, it is expected that contracting officers will not make an award, exercise an option or extend the period for performance of a contract, unless the contractor is compliant with the relevant CMMC level obligations.

To help determine the CMMC level that may apply to future contracts, contractors should begin by reviewing any current DOD contracts and programs — or prospective solicitations — to identify the types of information they handle.

Contractors that handle FCI — which includes information not intended for public release, provided by or generated for the federal government under a contract to develop or deliver a product or service — should be prepared to comply with at least CMMC Level 1 practices.

Contractors that store, process or transmit CUI should be prepared to comply with CMMC Level 2 or CMMC Level 3, depending on the sensitivity of the information and the criticality of the contractor's role in the DOD supply chain.

Where there are questions about the CMMC level that could apply to a future contract or program, particularly for those companies that may need CMMCLevel 3, contractors should consider reaching out to their agency contacts for more information about CMMC implementation.

Subcontractors, too, should review and assess any applicable CMMC requirements flowing down from the prime contract.

2. Account for all information systems supporting DOD contracts.

In addition to determining which CMMC level is likely to apply to future contracts, contractors should begin taking inventory of their information systems that support DOD contracts and track the type of information stored, processed or transmitted on those systems.

Covered information systems include all types of computing platforms that can process, store, or transmit CUI or FCI, and can include specialized systems — such as industrial and process-control systems — or physical devices.

When contractors report in SPRS, the DOD will provide unique identifiers for each contractor system. The proposed rule requires DOD contractors and subcontractors to specifically identify those information systems with CUI and FCI that will be used in performance of the contract. Thus, DOD contractors that haven't already done so need to inventory their systems, and prepare to report on all systems that support DOD contracts.

The Georgia Tech suit makes clear that the government is taking a serious look into whether contractors are properly accounting for all information systems that support DOD contracts.

One of the key claims brought by the DOJ alleges that Georgia Tech knowingly failed to include all covered equipment — including laptops, desktops and servers — in the scope of its system security plan.

To avoid increased scrutiny, contractors should get started as soon as possible to account for all information systems with CUI and FCI, including any specialized systems and devices, to plan for CMMC compliance.

3. Assess whether subcontractors and service providers are able to meet CMMC requirements.

Once live, CMMC certification requirements must be flowed down to subcontractors at all tiers when the subcontractor will process, store, or transmit FCI or CUI, based on the sensitivity of the information.

The DOD acknowledges that prime contractors do not have access to the SPRS database to confirm compliance by subcontractors, but primes are expected to verify subcontractor compliance. The proposed rule also specifically states that foreign suppliers are not exempt from these requirements.

It is likely that many subcontractors, especially smaller entities, may have to invest significant time and effort to achieve CMMC compliance. Thus, prime contractors should begin communicating with subcontractors about anticipated flow-downs now to make sure that subcontractors are not caught by surprise once CMMC phased implementation begins.

Subcontractors should generally anticipate that they will be subject to the same CMMC level or lower, depending on the sensitivity of the information needed to perform the subcontract.

Prime contractors should further consider how to verify that their subcontractors can meet the applicable CMMC requirements. While it is presently unclear how in-depth the DOD will expect primes to go to verify subcontractor compliance, especially at lower-tier subcontractor levels, contractors may consider reviewing system security plans and related documentation, or requiring subcontractors to submit a cyber questionnaire to show their capabilities.

Prime contractors and subcontractors alike might also consider participating in the DOD's Joint Surveillance Voluntary Assessment Program to show organizational capability to handle CUI. Participation in this program allows for the voluntary assessment to be converted into a three-year CMMC certification once the rulemaking goes into effect, and may also serve as a market differentiator from organizations competing for the same contracts.

Additionally, external service providers and cloud service providers that handle sensitive DOD information, or facilitate security protection assets — i.e., firewalls, spam filters etc. — likely will need to be included in the contractor's CMMC scoping.

External service providers, defined in the proposed rule as "external people, technology, or facilities that an organization utilizes for provision and management of comprehensive IT and/or cybersecurity services on behalf of the organization," must meet the CMMC level equal to or greater than the level required by the contract if CUI or security protection data is processed, stored or transmitted on the provider's assets.

Contractors may use a cloud service provider that meets the security requirements equivalent to the Federal Risk and Authorization Management Program's moderate or high baseline for CMMC Level 2 or 3.

4. Review and update internal policies, procedures and plans, as necessary.

Maintaining and affirming continuous compliance with security requirements identified in Title 32 of the Code of Federal Regulations, Part 170, is a key component of compliance with the newly proposed CMMC rule.

As a prerequisite to contract award, DOD contractors and subcontractors must have provided in SPRS an affirmation of continuous compliance with security requirements for each applicable information system. Thus, to further evidence of compliance with applicable security requirements, contractors should plan to keep relevant policies, procedures and plans up to date.

Certain requirements from the National Institute of Standards and Technology mandate that policies and procedures, such as system security plans, be updated on a periodic basis. To properly assess compliance with relevant NIST controls, contractors should (1) make sure there is a system security plan in place; (2) define a frequency to update the system security plan; and (3) ensure that the system security plan is updated in accordance with the defined frequency.

This, too, is a key area that the government is likely to continue closely monitoring. As an example, the Georgia Tech complaint-in-intervention alleges that Georgia Tech's Astrolavos Lab failed to develop and implement a NIST 800-171-required system security plan for several years after federal contract work began.

Once a system security plan was created, the DOJ alleges that the system security plan was only updated once in over four years, with nonsubstantive revisions.

Contractors should similarly review any existing policies and procedures, including security policies, CUI policies and incident-response plans to identify potential compliance gaps.

The proposed CMMC rule includes a new requirement that contractors report within 72 hours any "lapses in information security" or changes in the status of CMMC levels during contract performance. Contractors should make certain that there are organizational procedures in place to comply with these reporting requirements, in addition to other applicable incident reporting requirements.

Additional Considerations

In addition to the aforementioned key actions, contractors should consider submitting comments on the CMMC proposed rule. The 60-day public comment period is currently open until Oct. 15. Contractors and industry participants should submit written comments through the federal rulemaking portal by searching for "DFARS Case 2019-D041."

The DOD invites public comments on the following topics, in particular:

- Whether this collection of information is necessary for the proper performance of DOD functions, including whether the information will have practical utility;
- The accuracy of the DOD's estimated burden of information collection;
- Ways to enhance the quality, utility and clarity of information to be collected; and
- Ways to reduce the burden of information collection.

Townsend L. Bourne is a partner and the leader of the government business group and governmental practice cybersecurity and data protection team at Sheppard Mullin Richter & Hampton LLP.

Lillia J. Damalouji is an associate at the firm.

[1] https://www.federalregister.gov/documents/2024/08/15/2024-18110/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of.

[2] https://www.justice.gov/opa/pr/unturned-states-files-suit-against-georgia-institute-technology-and-georgia-tech-research#:~:text=The%20United%20States%20joined%20a%20whistleblower%20suit%20and%20filed%20a.

[3] https://www.justice.gov/opa/media/1364901/dl?inline.