New Cybersecurity Standards Will Impact Defense Contractors in November: 5 Steps to Ensure CMMC Compliance

Insights
9.12.25

Starting November 10, federal contractors that perform work with the Department of Defense will need to ensure they comply with a new cybersecurity framework. The Department of Defense (DoD) just amended the Defense Federal Acquisition Regulation Supplement on September 10 to incorporate contractual requirements related to the Cybersecurity Maturity Model Certification (CMMC) program. Unlike the previous framework, this version emphasizes continuous compliance, not just a one-time certification. This Insight summarizes the key takeaways and provides a five-step compliance gameplan for governmental contractors.

What is the CMMC Program?

It is the U.S. Department of Defense's framework for ensuring sensitive governmental data is protected. It has three levels of cybersecurity and aligns with the widely accepted NIST cybersecurity standards. These levels are:

Level 1: Basic Safeguarding of Federal Contract Information (FCI)

- Applies to contractors and subcontractors who process, store, or transmit FCI.
- Requires an annual self-assessment and annual affirmation of compliance.
- Requires compliance with the 15 security requirements in 48 CFR § 52.204-21 which includes security such as limiting access to information sections, performing real-time scans, and frequent patching.

Level 2: Broad Protection of Controlled Unclassified Information (CUI)

- Applies to contractors and subcontractors who process, store, or transmit CUI.
- Requires either a self-assessment or a Certified Third-Party Assessor Organization (C3PAO) assessment every three years, as specified in the solicitation.
- Requires annual compliance with the provisions of NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations) which includes extensive security requirements.

Level 3: Higher-Level Protection of CUI Against Advanced Persistent Threats

Level 3: Higher-Level Protection of CUI Against Advanced Persistent Threats

- Applies to contractors who process, store, or transmit high-value CUI, generally involving critical national security information. If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the associated prime contract has a requirement for the CMMC Status of Level 3, then the subcontractor must meet at least the Level 2 requirements.
- Requires achieving CMMC Status of Level 2 and undergoing an assessment every three years by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).
- Requires the same compliance with NIST SP 800-171 and adds in additional requirements under NIST SP 800-172 (Enhanced Security Requirements for Protecting Controlled Unclassified Information).

Key Takeaways

CMMC compliance will now be mandatory and a contractual requirement in DOD contracts. Contractors are required to maintain the required CMMC level for all information systems used in performing the contract that will process, store, or transmit FCI or CUI for the length of the contract.

- Solicitations and contracts will not be awarded if the contract and contractor do not have a current CMMC status and CMMC level.
- Each year, the affirming official must log into the Supplier Performance Risk System (SPRS) to certify compliance with its CMMC requirements.
- Before awarding the contract, the contracting officers must check SPRS to ensure that the contractor has a current CMMC status and that the CMMC status matches the work under the contract.

What About Subcontractors?

Many organizations assisting with governmental fall into the category of a subcontractor and not a prime contractor. Under the new rule, prime contracts are required to flow down CMMC requirements to all subcontractors that will process, store, or transmit FCI or CUI in performance of the subcontract. Subcontractors also have to submit affirmations of continuous compliance and the results of their self-assessments into SPRS.

What if My Organization is Not Fully in Compliance?

The revised rule allows for the use of Plans of Action and Milestones (POA&Ms), which allow for conditional CMMC status if the contractor meets certain but not all requirements. Instead of being disqualified, a contractor can document what it needs to fix, outline its improvements, and commit to implementing the improvements. POA&Ms are only available to Levels 2 and 3 and not for every security control.

What is the Phase-In Period?

The DoD is phasing in the CMMC program requirements over four phases.

Phase 1: Begins November 10, 2025

- Requires Level 1 and Level 2 CMMC status for contract award.
- The DoD may require C3PAO in place of Level 2 self for applicable DoD solicitations and contracts.

Phase 2: Begins November 10, 2026

- Adds mandatory C3PAO certification where applicable.
- Potentially adds Level 3 DIBCAC assessment for applicable contracts.

Phase 3: Begins November 10, 2027

- Enforces C3PAO for all new contracts and potentially adds Level 3 DIBCAC assessment for applicable contracts.

Phase 4: Begins November 10, 2028

- Enforces all requirements for all levels.

This phased approach will help contractors prepare for the new requirements. However, we recommend contractors begin implementing the necessary requirements as soon as possible as compliance is challenging and time consuming.

5 Compliance Recommendations

Here are five recommendations you should consider in order to prepare for this new era of cybersecurity compliance. If you need assistance in deploying these best practices, reach out to any attorney on our Data Protection and Cybersecurity team.

1. Review your contracts and bids

DoD contractors and subcontractors should review their current contracts in this space and begin to determine the applicable CMMC level.

2. Engage C3PAOs early if expecting Level 2 or Level 3

The capacity of C3PAOs and the DIBCAC (for Level 3) to handle the increased volume of requests is unknown – so engaging early is highly suggested.

3. Review your subcontracts

Review your subcontractors and determine whether they process, store, or transmit FCI or CUI and determine the level of CMMC compliance needed.

4. Conduct a risk assessment

Consider conducting a risk assessment with outside counsel under attorney-client privilege to determine the current gaps in your CMMC compliance program.

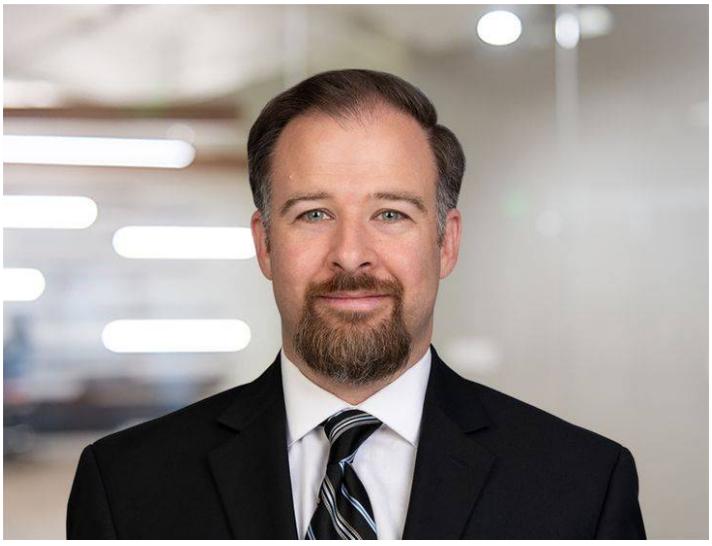
5. Data map your systems

Map which systems handle FCI or CUI.

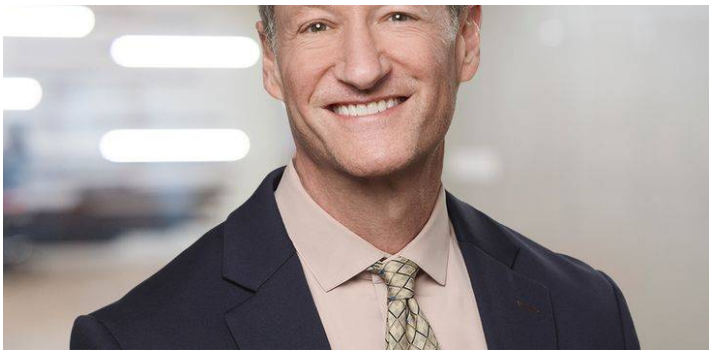
Conclusion

We'll continue monitoring developments and provide updates, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on our Data Protection and Cybersecurity team or in our Affirmative Action and Federal Contract Compliance group.

Related People



Kile E. Marks, FIP, CIPP/US, CIPM, CIPT
Associate
858.964.1582
Email



Daniel Pepper, CIPP/US
Partner
303.218.3661
Email

Jillian Seifrit, CIPP/US
Associate
610.230.6129
Email

Service Focus

Privacy and Cyber

Data Protection and Cybersecurity

Affirmative Action and Federal Contract Compliance