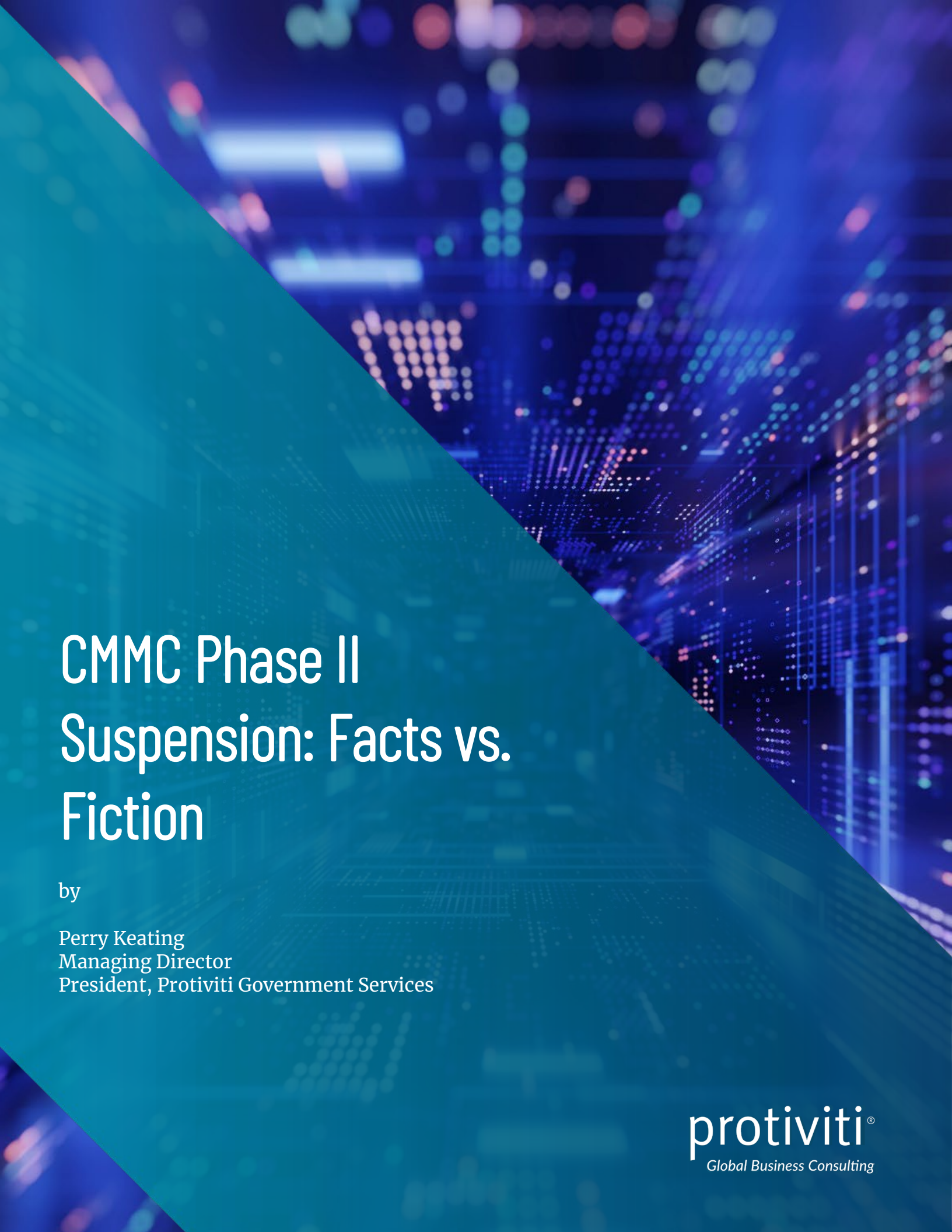


CMMC Phase II Suspension: Facts vs. Fiction

by

Perry Keating
Managing Director
President, Protiviti Government Services

protiviti®
Global Business Consulting

Executive summary

On July 13, 2026, the Department of Defense (DoD) announced the immediate suspension of CMMC Phase II implementation and established a 60-day CMMC Reform Task Force to conduct a comprehensive review of the programme. While this announcement creates uncertainty regarding the future of third-party certification requirements, organisation s should not interpret the decision as a relaxation of cybersecurity obligations.

The certification process may be changing. The requirement to protect government information is not. Self-assessments and SPRS reporting remain part of the current compliance framework.

Organisation s handling Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) remain subject to existing contractual cybersecurity obligations, including DFARS 252.204-7012 requirements, NIST SP 800-171 implementation expectations, self-assessment obligations, and related compliance activities. The DoD announcement affects the certification rollout timeline, not the underlying cybersecurity requirements.

The certification process may be changing. The requirement to protect government information is not. Self-assessments and SPRS reporting remain part of the current compliance framework.

Five things every contractor should know

1. **CMMC has not been cancelled.**

The CMMC programme remains active. The Department of Defense has paused the implementation of Phase II requirements and initiated a review of the programme. Phase I requirements remain in effect.

2. **NIST SP 800-171 remains in effect.**

Organisation s handling Controlled Unclassified Information (CUI) remain responsible for implementing and maintaining applicable NIST SP 800-171 security controls. These obligations are driven by existing contractual requirements and have not changed as a result of the Phase II suspension.

3. **DFARS cybersecurity requirements remain in force.**

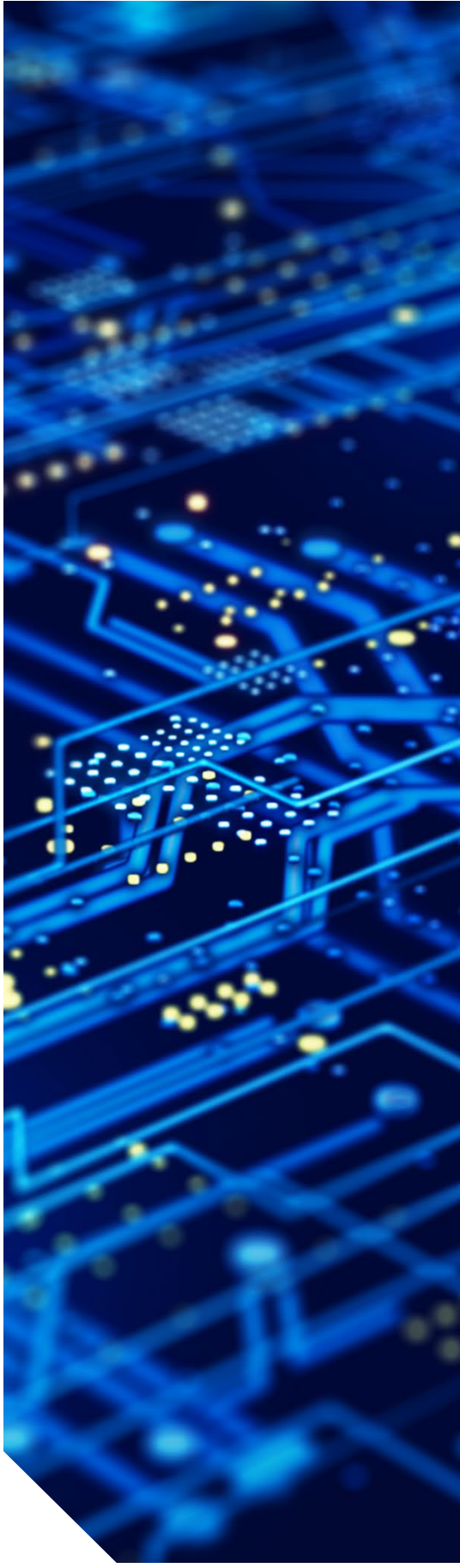
DFARS 252.204-7012 requirements continue to apply to covered defence information and remain contractually enforceable. These obligations are driven by existing contractual requirements and have not changed as a result of the Phase II suspension.

4. **False claims act exposure has not changed.**

Organisation s remain responsible for the accuracy of self-assessments, representations, affirmations, and cybersecurity compliance assertions made to the government.

5. **The certification timeline may change — cybersecurity obligations have not.**

The current discussion is about how cybersecurity compliance is verified, not whether cybersecurity is required.



Facts vs. fiction

Fiction	Fact	Key point
"CMMC has been canceled."	CMMC has not been canceled. The Department of Defense has suspended the Phase II rollout and launched a review of the programme. Phase I requirements remain in effect.	**Think "pause," not "cancel."** The CMMC programme remains active while DoD evaluates potential reforms.
"We no longer need to comply with NIST SP 800-171."	NIST SP 800-171 requirements remain in place and continue to form the basis for protecting Controlled Unclassified Information (CUI).	**The security requirements remain.** Organisation s handling CUI must continue implementing and maintaining required controls.
"DFARS cybersecurity requirements are gone."	DFARS 252.204-7012 requirements remain fully enforceable. Contractors are still required to protect covered defence information.	**Contractual obligations have not changed.** The requirement to protect government information remains.
"We should stop our cybersecurity improvement efforts."	Organisation s should continue executing their cybersecurity roadmap and remediation activities.	**Continue the journey.** Strong cybersecurity remains essential regardless of how the certification process evolves.
"All of our CMMC preparation work was wasted."	Readiness efforts remain valuable and continue to support compliance, audit readiness, cybersecurity maturity, and operational resilience.	**Keep building.** SSPs, POA&Ms, policies, procedures, evidence repositories, and security improvements still matter.
"The government is backing off cybersecurity."	Cybersecurity remains a top priority for the DoD. The review focuses on certification processes and administrative burden—not security expectations.	**Cybersecurity is still the mission.** The discussion is about how compliance is verified, not whether security is required.

Fiction	Fact	Key point
"The government is accepting self-attestations again, so audit readiness no longer matters."	Organisation s remain responsible for demonstrating compliance and supporting self-assessment assertions with appropriate evidence.	**Evidence still matters.** Documentation, policies, procedures, technical artifacts, and audit trails remain critical.
"If CMMC changes, we no longer need to identify and protect CUI."	Organisation s that receive, process, store, or transmit CUI remain responsible for protecting that information.	**The data did not change.** Understanding where CUI resides and how it is protected remains fundamental.
"The DOJ will stop pursuing cybersecurity enforcement cases."	False Claims Act exposure and DOJ Civil Cyber-Fraud Initiative enforcement remain unchanged.	**Be careful what you attest to.** Companies must be able to support compliance claims with evidence.
"SPRS scores are no longer important."	Self-assessments and SPRS reporting remain part of the current compliance framework.	**Maintain accurate records.** Organisation s should continue managing SPRS scores, documentation, and affirmations.
"Existing contracts with CMMC requirements will stay as-is."	The DoD has indicated that certain solicitations and contracts containing CMMC certification requirements may be amended during the review period.	**Review your contracts carefully.** Monitor modifications and guidance from contracting officers.
"Small businesses can just wait until the government decides what to do."	The Reform Task Force is expected to deliver recommendations within 60 days, and future requirements may evolve quickly.	**Use this time wisely.** Stay informed, improve cybersecurity, and maintain readiness for future changes.
"CMMC is over."	The certification process is temporarily paused, but cybersecurity requirements remain in force.	**Continue protecting CUI and FCI.** The security mission remains unchanged.

What has not changed

Organisation s should continue to:

- Protect Federal Contract Information (FCI).
- Protect Controlled Unclassified Information (CUI).
- Comply with DFARS 252.204-7012 requirements.
- Maintain NIST SP 800-171 compliance efforts.
- Perform required self-assessments.
- Maintain and update System Security Plans (SSPs).
- Maintain Plans of Action & Milestones (POA&Ms).
- Maintain accurate SPRS submissions and affirmations.
- Continue cybersecurity remediation activities.
- Prepare for potential government-led reviews and audits.
- Maintain defensible cybersecurity documentation and evidence repositories.
- Maintain incident response, logging, monitoring, and vulnerability management capabilities.
- Continue identifying and protecting CUI throughout the enterprise.
- Ensure executive affirmations and compliance representations are supportable and evidence-based.

What should contractors do now?

Organisation s should consider the following actions during the review period:

- Continue NIST SP 800-171 implementation and remediation efforts.
- Maintain current SSPs, POA&Ms, policies, procedures, and supporting evidence.
- Validate SPRS submissions and annual affirmations.
- Continue identifying, classifying, and protecting CUI and FCI.

- Review active solicitations and contracts for potential modifications.
- Evaluate cybersecurity representations made to customers and government agencies.
- Continue preparing for potential future certification, assessment, or audit requirements.
- Monitor guidance issued by the DoD CIO and CMMC Reform Task Force.
- Avoid making business decisions based on assumptions that cybersecurity requirements have been relaxed.
- Use this period to mature cybersecurity capabilities and close known security gaps.

What may change

The following areas are currently under review:

- Future role of independent third-party assessments (C3PAOs)
- Timing of future implementation phases
- Assessment methodologies
- Certification requirements for various contractor populations
- Approaches intended to reduce burden on small and non-traditional businesses
- Alternative cybersecurity verification models
- Potential updates to assessment and attestation processes
- Future alignment between certification activities and cybersecurity outcomes

Protiviti's perspective

As a CyberAB Registered Practitioner Organisation (RPO), we believe organisation s should remain focused on the fundamentals. Cybersecurity compliance should not be viewed solely as a certification exercise. It is a business, operational, contractual and national security requirement.

The certification model may evolve over the next 60 days, but the obligation to protect government information remains unchanged. Organisation s that continue investing in governance, cybersecurity controls, documentation, evidence management, continuous monitoring, and operational resilience will be best positioned regardless of the outcome of the Department of Defense review.

Companies that use this period to strengthen cybersecurity programmes, improve documentation, close known control gaps, enhance executive oversight and improve audit defensibility will be positioned to respond effectively regardless of the future direction of the CMMC programme.

Cybersecurity compliance should not be viewed solely as a certification exercise. It is a business, operational, contractual and national security requirement.

About Protiviti Government Services

Protiviti Government Services is a CyberAB Registered Practitioner Organisation (RPO) that assists organisation s with CMMC, NIST SP 800-171, DFARS, Government Data Protection, Compliance Readiness, Cybersecurity Programme Management, Technical Remediation, and AI-enabled compliance acceleration services.

For additional information regarding CMMC readiness, cybersecurity compliance and government data protection services, please contact CMMC@protiviti.com.

About the author

Perry Keating
Managing Director & President, Protiviti Government Services

Mr. Keating is the Managing Director and President of Protiviti Government Services with over 30 years of doing business with the government and the Defense Industrial Base (DIB). His experience gives him unique industry insight into the Public Sector (US Federal, State & Local), Aerospace & Defense (A&D), Government Contractors (GovCon), Defense Industrial Base (DIB), as well as the Telecommunications and High-Tech industries.