Kiteworks

EXECUTIVE SUMMARY

State of CMMC 2.0 Preparedness in the DIB — Executive Summary

THE PHASE II SUSPENSION: THE DEFENSE INDUSTRIAL BASE KEPT MOVING, BUT CONFIDENCE IS OUTRUNNING EVIDENCE

Overview

On July 13, 2026, the Department of War suspended CMMC 2.0 Phase II third-party assessments.[1] This report answers the question that suspension raised: did the market pause with it, or keep moving? Kiteworks surveyed 273 Defense Industrial Base organizations in the days immediately after the announcement, every respondent confirmed they do business with the DoW and must meet a CMMC 2.0 Level 1, 2, or 3 requirement. It is one of the first survey reads of what the DIB actually did once the rules shifted under it, rather than a forecast of what it might do.

The short answer: the market did not pause. 98% of surveyed organizations took at least one concrete action in response. Only 2% did nothing. But "kept moving" and "ready" are not the same thing, and the distance between them is where the risk now sits.

Because self-reported confidence is a poor measure of readiness, this report scores each organization on verifiable facts rather than feelings. Two composite indices, each built from eight binary yes/no indicators drawn from the survey, anchor the analysis:

CMMC Compliance Maturity Score (CCMS)	Eight indicators of where an organization's compliance program stands today, expressed as a 0–100 index. The survey mean is 78.2, roughly 6.3 of 8 indicators in place.
Suspension Governance Score (SGS)	Eight indicators of active behavior since July 13, on the same 0–100 scale. The survey mean is 74.9, roughly 6.1 of 8 indicators in place.
CMMC Suspension Readiness Index (CSRI)	CCMS × (SGS/100). The survey mean is 60.0 out of 100, median 65.6. The index multiplies rather than averages: a strong compliance record cannot compensate for a passive response, and a busy response cannot compensate for a weak compliance foundation. Averaging the two means would produce roughly 77; multiplying gives 60.0, and that difference is the point.

What the arithmetic makes visible is the minority the headline resilience hides: 31% of this already-qualified population, more than one organization in four, scores low on both dimensions at once. That group, not the majority already ahead of it, is who this report is written for.

The Suspension Paused the Due Date, Not the Law

The pause did not touch the underlying obligation. DFARS clause 252.204-7012 still requires contractors handling covered defense information to implement NIST SP 800-171 and self-report a score to the Supplier Performance Risk System.[2] Phase 1 self-assessment requirements remain in effect.[3] The False Claims Act still applies to that score.[4] Phase II was the independent-verification layer sitting on top of the obligation; removing it does not remove the obligation, it removes the check on whether a contractor's own claim about its compliance is true.

The Department of Justice has already given the DIB a preview of what an inaccurate self-attestation costs. In June 2026, a defense contractor, LOGZONE Inc., settled a False Claims Act case for $507,144.[5] It had self-attested a perfect SPRS score of 110; a government audit later assessed the real figure at −170. No whistleblower was involved. A routine government audit surfaced the gap, and those audits are still running during the suspension. 84% of the contractors surveyed are concerned about exactly this exposure, and 92% have already engaged legal or compliance review to check it.

How the Scores Are Built

Both indices are computed from binary, checkable facts rather than self-rated confidence. That distinction matters, because this report's own data shows confidence and evidence diverging sharply, and a self-assessment score would sit well above what most organizations can demonstrate.

The CCMS sums eight indicators of current compliance state, with the share of respondents meeting each:

CCMS Indicator	% Meeting
Self-assessment substantially or fully compliant	88%
SPRS score submitted and current	59%
Has engaged a C3PAO for Level 2+ assessment	96%
Fully aware DFARS 252.204-7012 shapes strategy	73%
Does not hold the "all requirements paused" misconception	97%
Meaningful budget committed ($150,000 or more)	86%
Legal/compliance review conducted since the suspension	92%
Already using a FedRAMP-authorized platform	35%

The single weakest CCMS indicator, by a wide margin, is FedRAMP-authorized platform adoption at 35%.

The SGS sums eight indicators of active governance behavior since July 13:

SGS Indicator	% Meeting
Continued implementing technical controls as planned	62%
Budget not decreased or paused since the suspension	88%
Internal priority maintained or increased	89%
Communicated with primes/subs about flow-down	62%
Actively evaluating new compliance tools or platforms	51%
Plans to submit comments on DoW's RFI	93%
Has a specific 60–90 day action plan	99%
Actively strengthening self-attestation documentation	55%

The weakest SGS indicator is active evaluation of new compliance tooling at 51%.

The Readiness Framework Quadrants

Mapping CCMS against SGS produces four quadrants that are more diagnostic than either score alone. A flat midpoint threshold is too lenient for this pre-qualified population; at a 7-of-8 threshold on each dimension, the split is genuinely differentiated:

Quadrant	Profile	% of Quadrant
Audit-Ready	Strong compliance state and active governance together	23%
Coasting	Compliant on paper, passive in practice	28%
Scrambling	Behaviorally active without the compliance foundation	18%
Exposed	Weak on both dimensions at once	31%

Exposed is the single largest quadrant, at 31% of an already-qualified, already-engaged population. Only 2% score a perfect 8 of 8 on both dimensions at once. This is the distribution behind the survey mean CSRI of 60.0.

The Confidence–Evidence Cascade

The central finding sits underneath those quadrants: confidence is not evidence. 96% of respondents are confident their self-attested SPRS score would hold up if reviewed today. Follow that same confident group one step at a time, and the number falls sharply.

The Confidence–Evidence Cascade	% of Respondents
Confident their SPRS score would hold up under review	96%
… of those, SPRS submission is current	60% (of 96%)
… of those, already on a FedRAMP-authorized platform	36% (of 96%)
… of those, can point to BOTH a current score and an audited platform	29% (of 96%)

Fewer than three in 10 of the organizations that call themselves confident can fully back it. Each row is what should stand behind the row above it. Confidence outruns evidence at every stage of this cascade, and that gap is the report.

Key Findings

1

Preparedness Didn't Pause

98% took at least one concrete action; only 2% did nothing. 62% continued implementing technical controls as planned, and 49% reallocated CMMC-related budget, but reallocation was lateral, not a retreat: of redirected budget, 63% went to independently audited (FedRAMP) platforms and 55% to expanded audit-logging and evidence generation, with only 4% reporting no reallocation at all. The suspension redirected the market. It did not pause it.

2

The Confidence Illusion

Only 3% believe every CMMC requirement is paused, so awareness that something survived is near-universal. Component knowledge is thinner: 48% do not know Phase 1 self-assessment obligations continue, and 57% do not know select government-led assessments continue. Self-reported confidence barely tracks this knowledge, scoring against four factual items, "very confident" respondents average 2.48 of 4, statistically indistinguishable from the 2.48 average among the merely "somewhat confident," and 49% of the "very confident" scored below 3 of 4. Understanding the suspension does not calm legal concern; it sharpens it. 57% of organizations fully confident in their understanding are very concerned about False Claims Act exposure, against 20% of those only somewhat confident.`

3

Legal and Regulatory Exposure

84% are concerned about False Claims Act exposure from an inaccurate self-attested SPRS score, and 92% have engaged legal or compliance review since the suspension. Among the weakest-compliance-status organizations in the survey, 80% are nonetheless confident their score would hold up, confidence detached from the underlying state. Asked what would most increase that confidence, respondents point to evidence, not paperwork: 47% name a complete real-time audit trail and 36% name independent third-party (FedRAMP) authorization, against only 11% naming a legal review. Flow-down concern is high and concentrates where privity is weakest: 86% overall, rising to 92% among Tier 1 subcontractors and 89% among Tier 2-or-lower, against 79% among prime contractors.

4

Market Consequences Are Already Visible

55% are now bidding on solicitations they previously would have avoided over Level 2 requirements, and 52% have withdrawn from a bid rather than pursue certification, both effects live in the same population. 38% report losing or being disqualified from a contract over a Level 2 requirement, and those losses fall hardest on the least-leveraged part of the supply chain: Tier 2-or-lower subcontractors report a bid loss at 55%, nearly double the 31% rate among prime contractors. Aerospace and Defense Manufacturing is the most insulated industry, though less so than an earlier data pull suggested, at a 16% loss rate.

5

Assessor and Platform Priorities

Demand has moved to independently audited infrastructure: 89% of respondents are already using, or plan to adopt within six months, a FedRAMP-authorized platform, and 93% say independent third-party authorization will be essential or important to future vendor selection. On the assessor side, 96% have engaged a C3PAO at some point and 32% are continuing a scheduled assessment voluntarily, with no deadline compelling them to. The two needs are complementary, not competing: the DIB wants evidence-generating technology to support its self-attestation and an independent assessor to validate the posture that technology documents.

Cross-Analyses: Variations by Key Factors

By Industry

Aerospace and Defense Manufacturing leads the CSRI distribution at 66.2, followed by Information Technology and Cloud Services at 61.9 and Telecommunications and Critical Infrastructure at 59.3, with the combined Other Industries bucket trailing at 52.2. The industry rank order tracks the bid-outcome insulation seen in the market findings.

By DIB role

Organizations that are both a prime and a subcontractor score highest on CSRI at 64.7, ahead of pure primes at 61.6. Tier 1 and Tier 2-or-lower subcontractors sit together near the bottom at 52.1 and 52.2, the least-leveraged and least-ready segment, and the one absorbing the most bid loss.t

By Region

North America (60% of the sample) posts a mean CSRI of 64.7; Europe (38%) posts 53.9, an 11-point gap and the largest single regional divergence in the report. European DIB entities face the same US-DoW self-attestation obligations as their North American peers, from a measurably weaker starting posture.

By Organization Size

CSRI is not strictly monotonic with size. The 1,000-4,999 band scores highest at 64.2, while the largest organizations (5,000+) score below it at 57.8, consistent with the finding that the largest enterprises communicate with primes and subs about flow-down at far below the overall rate. The smallest organizations (50-249) score lowest at 51.9, an under-resourced profile rather than a deprioritizing one.

Implications and Recommendations

The strategic implication is direct. The suspension changed who checks the math, not what the math has to add up to. DFARS 252.204-7012, the NIST SP 800-171 obligation, and the DOJ's Civil Cyber-Fraud Initiative all remained in force. An organization that treats the pause as license to slow down is not avoiding cost. It is deferring risk into a period with less independent verification standing between a self-attestation and a False Claims Act referral, not more. For leadership, the 31% of this population scoring low on both dimensions is not a fringe segment; it is more than a quarter of an already-qualified DIB, and a legal exposure that predates the suspension does not wait for a policy review to conclude.

The operational path has two complementary tracks, because no single move closes the confidence-evidence gap.

1

The Platform Track

The single weakest CCMS indicator is FedRAMP-authorized platform adoption at 35%; the weakest SGS indicator is active evaluation of new compliance tooling at 51%. Both are addressable through procurement now, not by waiting on the Reform Task Force.6 Organizations should prioritize independently audited, evidence-generating secure data exchange capable of producing the audit trail 47% of respondents already say would most increase confidence in their own self-attestation, turning a confident claim into a defensible, provable one.

2

The Assessment Track

96% of respondents have already engaged a C3PAO, and 32% are continuing a scheduled assessment voluntarily. Organizations sitting on a paused or cancelled assessment should treat voluntary continuation as the default, not the exception it already is for nearly a third of the DIB. A completed independent assessment produces exactly the validation the confidence-evidence gap shows self-attestation alone cannot provide. Evidence plus independent validation is what turns a confident attestation into a defensible one.

Conclusion

The Defense Industrial Base did not wait. 98% of surveyed organizations took concrete action after the July 13 suspension, budget moved toward compliance infrastructure rather than away from it, and 93% plan to participate in shaping what CMMC becomes next. That is the headline, and it is arithmetic, not optimism.

It is not the whole picture. More than a quarter of this already-engaged population scores low on both compliance state and active governance at once, and fewer than three in ten organizations that call themselves confident in their self-attested SPRS score can back that confidence with both a current submission and an independently authorized platform. The suspension removed a verification requirement. It did not remove the obligation that requirement existed to check, and the DOJ's own recent enforcement record shows the gap does not need a whistleblower to surface.

This report's CCMS, SGS, and CSRI framework establishes a 2026 baseline. A future wave can measure whether the gap it documents closes or widens, and whether the organizations in the Exposed quadrant move, or stay where they are.

Endnotes

1. U.S. Department of War, "Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements," press release, July 13, 2026, See also Justin Doubleday, "Pentagon Suspends CMMC Phase Two Requirements, Launches Review of Program," Federal News Network, July 13, 2026.

2. Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting,"; National Institute of Standards and Technology, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST Special Publication 800-171 Rev. 2 (February 2020, updated January 28, 2021).

3. Alexander B. Hastings, Daniel Funaro, Scott Whitman, Moshe Klein, and Alison Tanchyk, "Department of War Suspends CMMC Phase II Requirements, but Cybersecurity Obligations Remain," Morgan Lewis LawFlash, July 16, 2026.

4. Michelle A. Freeman, Matthew D. Krueger, Jason Mehta, and Joseph W. Swanson, "DOJ's LOGZONE Settlement Highlights FCA Risk in Cybersecurity Compliance Representations," Foley & Lardner LLP, July 6, 2026; on the enforcement program itself, U.S. Department of Justice, Office of Public Affairs, "Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative," press release no. 21-971, October 6, 2021.

5. U.S. Department of Justice, Office of Public Affairs, "Alabama Defense Contractor Agrees to Pay $507,144 to Resolve False Claims Act Liability Relating to Cybersecurity Violations," press release no. 26-676, June 18, 2026.

6. WilmerHale, "Pentagon Suspends CMMC Phase 2 Requirements and Launches Review of Cybersecurity Certification Program," client alert, July 20, 2026; ; Office of the Department of War Chief Information Officer, "CMMC Reform Memorandum," July 13, 2026.