Kiteworks

ANNUAL SURVEY REPORT

State of CMMC 2.0 Preparedness in the DIB

The Phase II Suspension: Readiness, Risk, and the Confidence Gap Across the Defense Industrial Base

Contents

LETTER FROM THE EDITOR

The Suspension Paused the Audit Deadline. It Did Not Pause the Defense Industrial Base.

On July 13, 2026, the Department of War suspended CMMC 2.0 Phase II third-party assessments.[1] Did that suspension change the market — did it show up in bidding, budgets, and behavior, or only in headlines? And separately: how ready is the Defense Industrial Base for CMMC, whenever Phase II resumes? This report answers both questions with data from 273 confirmed DoW-business organizations surveyed in the days after the announcement, not with speculation about what a suspension probably means.

The short answer to the first question: yes, and not the way most coverage assumed. 98% of surveyed organizations took at least one concrete action in response to the suspension. Only 2% did nothing. Budget reallocation moved toward compliance infrastructure, not away from it. The market did not pause. It redirected. The short answer to the second question: unevenly, and this report is built to show exactly where. To measure readiness precisely rather than by feel, we built two indices directly from this survey's own questions. The CMMC Compliance Maturity Score (CCMS) is built from 8 binary facts about where an organization's compliance program stands today — is the self-assessment documented, is the SPRS score current, has a C3PAO been engaged, and five more. Each organization earns one point per fact that is true, out of 8, normalized to a 0–100 index. The survey mean is 78.2. That means the average organization has 6.3 of 8 facts in place — a count of specific, checkable things, not a rounded average of how confident people feel.

The Suspension Governance Score (SGS) uses the same construction — 8 binary facts, this time about what the organization did after July 13: kept building technical controls, communicated with its supply chain, began evaluating new tooling, and five more. The survey mean is 74.9.

What matters is what happens when the two are combined. We multiply them, not average them: CSRI = CCMS × (SGS ÷ 100). At the survey means, that comes to 60.0 — not the roughly 77 a simple average would produce. That is not a design flaw. A strong compliance record does not make up for a passive response to the suspension, and a busy response does not make up for a weak compliance record underneath it. Multiplication is what forces a real readiness score to earn both halves rather than average around a weakness.

What that arithmetic makes visible is the minority the headline number hides: 29% of this survey's population — already confirmed to do business with the DoW, already carrying a live CMMC requirement — scores low on both dimensions at once. That is the group this report is written for as much as the majority already ahead of it.

Patrick Spencer, Ph.D.
SVP, Americas Marketing & Industry Research, Kiteworks

Executive Summary

Two questions bring most readers to this report. Did the July 13, 2026 suspension of CMMC 2.0 Phase II third-party assessments change how the Defense Industrial Base operates — in bidding, budgets, and day-to-day behavior — or only in how it was covered? And separately, regardless of the suspension: how ready is the DIB for CMMC compliance today? This survey of 273 confirmed DoW-business organizations, fielded July 17–31, 2026, answers both directly, with numbers rather than impressions.

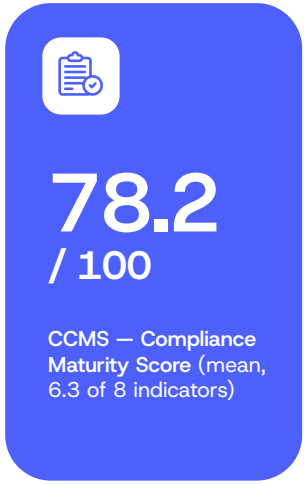
The answer to the first question: yes, the suspension changed real behavior, immediately and measurably. 98% of respondents took at least one concrete action in response.

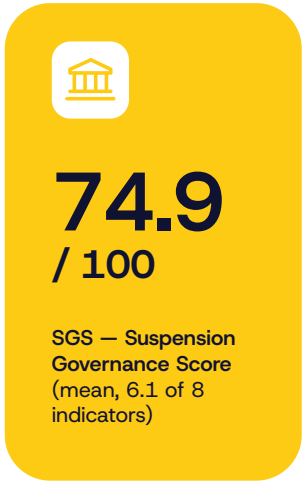
2% did nothing.

The answer to the second question — how ready the DIB actually is — isn't a single number a survey can simply ask for. Self-reported confidence, as this report's own data shows later, does not reliably track readiness. So instead of asking organizations to rate themselves, this report builds two composite scores directly from specific, checkable facts each respondent reported about their own organization. The CMMC Compliance Maturity Score (CCMS) counts 8 such facts about current compliance state — is the self-assessment documented, is the SPRS score current, has a C3PAO been engaged, is there a budget of at least $150,000 committed, and four more — and expresses the count as an index from 0 to 100, where 100 would mean all 8 facts are true. The Suspension Governance Score (SGS) does the same for 8 facts about active behavior specifically since July 13 — did the organization keep building technical controls, communicate with its supply chain about flow-down, begin evaluating new compliance tooling, and five more.

Combining the two into a single readiness number requires a choice, and this report multiplies rather than averages: CCMS × (SGS ÷ 100). The reason is practical, not statistical. Averaging would let an organization with a strong compliance record and a completely passive response to the suspension still land in the middle of the scale — as would an organization busily taking action with no underlying compliance foundation to show for it. Multiplying does not allow either shortcut: a low score on either dimension pulls the combined score down regardless of how high the other one is. The result is the CMMC Suspension Readiness Index (CSRI). The next section of this report, The CMMC Readiness Framework, gives the complete formula, all 16 underlying indicators, and every tier boundary in full — this summary gives the headline numbers that framework produces.

The Readiness Framework, In Numbers





CMMC Suspension Readiness Index (CSRI): 60.0 / 100

The index is multiplicative: CSRI = CCMS × (SGS / 100). A strong compliance record does not make up for a passive response to the suspension, and an active response does not make up for a weak compliance record underneath it. 29% of this survey's population — already confirmed to do business with the DoW, already carrying a live CMMC requirement — scores low on both dimensions simultaneously. That group is who this report is written for.

Confidence and evidence diverge further than the headline number suggests. 96% of respondents say they are confident their self-attested SPRS score would hold up if reviewed today. Follow that same group one step further and the picture changes.

The Confidence-Evidence Gap, In One View

Confident their SPRS score would hold up under review	96%
Of those, SPRS submission is current	60%
Of those, already on a FedRAMP-authorized platform	36%
Of those, have both a current SPRS score and a FedRAMP platform	29%

Roughly three in ten of the organizations that call themselves confident can back it with both a current SPRS submission and a FedRAMP-authorized platform. Each row is the evidence that should stand behind the row above it; confidence is not the same as evidence at any stage of this cascade.

That gap carries legal weight. DFARS clause 252.204-7012 never paused[2] — the suspension removed the third-party check on self-attestation, not the underlying obligation to attest accurately.[3] The Department of Justice's June 2026 settlement with LOGZONE Inc., a $507,144 False Claims Act case built from a routine government audit rather than a whistleblower complaint, is the closest thing this survey has to a preview of what an inaccurate SPRS score costs.[4] 84% of respondents say they are concerned about exactly that exposure, and 92% have already engaged some form of legal review to check it.

Prior Wave Check — What Changed Since March 2025

The Kiteworks "Data Security and Compliance Risk: 2025 State of CMMC Preparedness in the DIB Report," a March 2025 survey of 209 Defense Industrial Base organizations, found budget and resource constraints to be the single most-cited CMMC compliance challenge, at 36%.[5]

Following the Phase II suspension, budget concern has dropped to second place at 22%. The top concern is now flow-down pressure from primes, at 26%.

The compliance bottleneck moved from a resourcing problem to a relationship problem.

The market has not paused on the commercial side either. 55% are now bidding on solicitations they would previously have avoided over Level 2 requirements. 52% have also withdrawn from a bid rather than pursue certification, and 38% report losing or being disqualified from a contract over the same requirement. Both effects are live in the same population. The suspension opened a door for some and closed one for others, and which side an organization lands on has little to do with the suspension itself.

93% plan to comment on DoW's Request for Information, due August 14, 2026.[6] 58% expect Phase II to return in a modified form; only 4% think it disappears outright. The rest of this report builds out the CCMS/SGS/CSRI framework in full, breaks the confidence gap down by segment, and closes with a self-scoring checklist any DIB organization can run against its own numbers.

Over half of respondents indicate they withdrew from a DoW bid rather than pursuing certification this past year.

Almost 4 in 10 respondents revealed they lost a bid or were disqualified from one due to the lack of CMMC 2.0 certification in the last year.

About the Survey

This report is based on primary research conducted with 273 security, compliance, risk management, and IT leaders at organizations confirmed to do business with the Department of War and to carry an active CMMC 2.0 Level 1, 2, or 3 requirement. The survey was fielded July 17–31, 2026, in the days immediately following the July 13, 2026 suspension of CMMC 2.0 Phase II third-party assessments.

The survey covered nine primary topic domains: awareness and understanding of the suspension; current compliance and self-assessment status; C3PAO engagement status; budget and priority impact; actions taken since the announcement; legal and False Claims Act exposure; bid and market consequences; vendor and secure data exchange priorities; and forward-looking plans, including RFI participation and expected Reform Task Force outcomes.[7] Responses were collected via an online survey platform; all findings are self-reported by survey participants. Figures reflect the share of 273 respondents unless otherwise noted, and a small number of individual questions carry a slightly different base where a respondent skipped that item.

Survey Demographics

Industry Sector	% of respondents
Information Technology & Cloud Services	45%
Telecommunications & Critical Infrastructure	17%
Aerospace & Defense Manufacturing	16%
Other Industries*	21%

Combines six different industries that had less than 5% of the respondents each: professional services, manufacturing, higher education, healthcare, retail, and logistics and transportation.

Employee Numbers	% of respondents
5,000 or more employees	14%
1,000 to 4,999 employees	42%
500 to 999 employees	27%
250 to 499 employees	11%
50 to 249 employees	5%

CMMC 2.0 Level	% of respondents
Level 3 (Expert)	64%
Level 2 (Advanced)	32%
Level 1 (Foundational)	2%
Don't know / not yet determined	1%

Prime or Sub Contractor	% of respondents
Both a prime and a subcontractor	36%
Prime contractor	34%
Subcontractor (Tier 1)	15%
Subcontractor (Tier 2 or lower)	14%

Region	% of respondents
North America	60%
Europe	38%

Role/Job Responsibility	% of respondents
CIO / IT Director or Manager	39%
CISO / IT Security Director or Manager	33%
CEO / Owner / President	16%
Program Manager / Contracts Manager	5%
Compliance Officer / DFARS Compliance Manager	4%
General Counsel / Legal	1%

The CMMC Readiness Framework

Two composite scores anchor the analysis in this report. The CMMC Compliance Maturity Score (CCMS) measures where an organization's compliance program stands today — a state, built from facts about certification status, budget, and legal posture that mostly cannot change overnight. The Suspension Governance Score (SGS) measures how actively an organization is governing itself through the ambiguity the suspension created — a behavior, built from actions an organization is choosing to take or not take right now. A third measure, the CMMC Suspension Readiness Index (CSRI), combines both into a single number. Together they give a three-dimensional picture of readiness that is reproducible, comparable across segments, and grounded in specific, verifiable survey responses rather than self-reported confidence.

CMMC Compliance Maturity Score (CCMS)

CCMS is a composite score expressed as an index from 0 to 100, computed from 8 binary indicator variables measured in this survey. Each indicator is scored 1 (in place) or 0 (not in place). CCMS is the sum of all 8 binary scores for each organization, normalized to a 0–100 index.

$$CCMS = \Sigma(c_1 \ldots c_8) / 8 \times 100$$

Where each $c^n \in \{0, 1\}$ and the 8 indicators are:

Indicator	% of respondents
c1 — Self-assessment substantially or fully compliant	88%
c2 — SPRS score submitted and current	59%
c3 — Has engaged a C3PAO for Level 2+ assessment	96%
c4 — Fully aware DFARS 252.204-7012 shapes compliance strategy	73%
c5 — Does not hold the "all requirements paused" misconception	97%
c6 — Meaningful budget committed, ≥$150,000	86%
c7 — Legal/compliance review conducted since the suspension	92%
c8 — Already using a FedRAMP-authorized platform	35%

Survey mean CCMS: 78.2 out of 100 — the average organization has 6.3 of 8 indicators in place. The lowest-deployed indicator by a wide margin is c8: roughly a third of respondents are already running on a FedRAMP-authorized platform. That gap is the single most specific, most actionable item this index surfaces.

Establishing the 2026 Baseline

CCMS and SGS are new measures, built specifically for this survey. No prior wave has measured either index, so there is no year-over-year comparison to draw on the framework itself — this report establishes the baseline that a future wave could measure against. Where this report can compare to prior Kiteworks CMMC research, it does so on specific, matched themes rather than on these two indices — for example, the shift in the DIB's top compliance concern since the March 2025 study.

Suspension Governance Score (SGS)

SGS uses the same construction as CCMS — 8 binary indicators, summed and normalized to a 0–100 index — but measures active behavior since July 13, 2026, rather than current state.

$$SGS = \Sigma(s_1 \ldots s_8) / 8 \times 100$$

Survey mean SGS: 74.9 out of 100 — 6.1 of 8 indicators in place. The lowest-deployed indicator is s5: just over half of respondents are actively evaluating new compliance tooling, the one behavior most easily influenced by vendor outreach and industry events.

Each indicator (s_n) is scored as a simple yes-or-no — 1 if the organization did it since the suspension, 0 if it did not — and SGS is the sum of the eight, scaled to a 0–100 index, so meeting all eight scores 100 and meeting four scores 50. The eight behaviors measured since July 13, and the share of respondents reporting each, are:

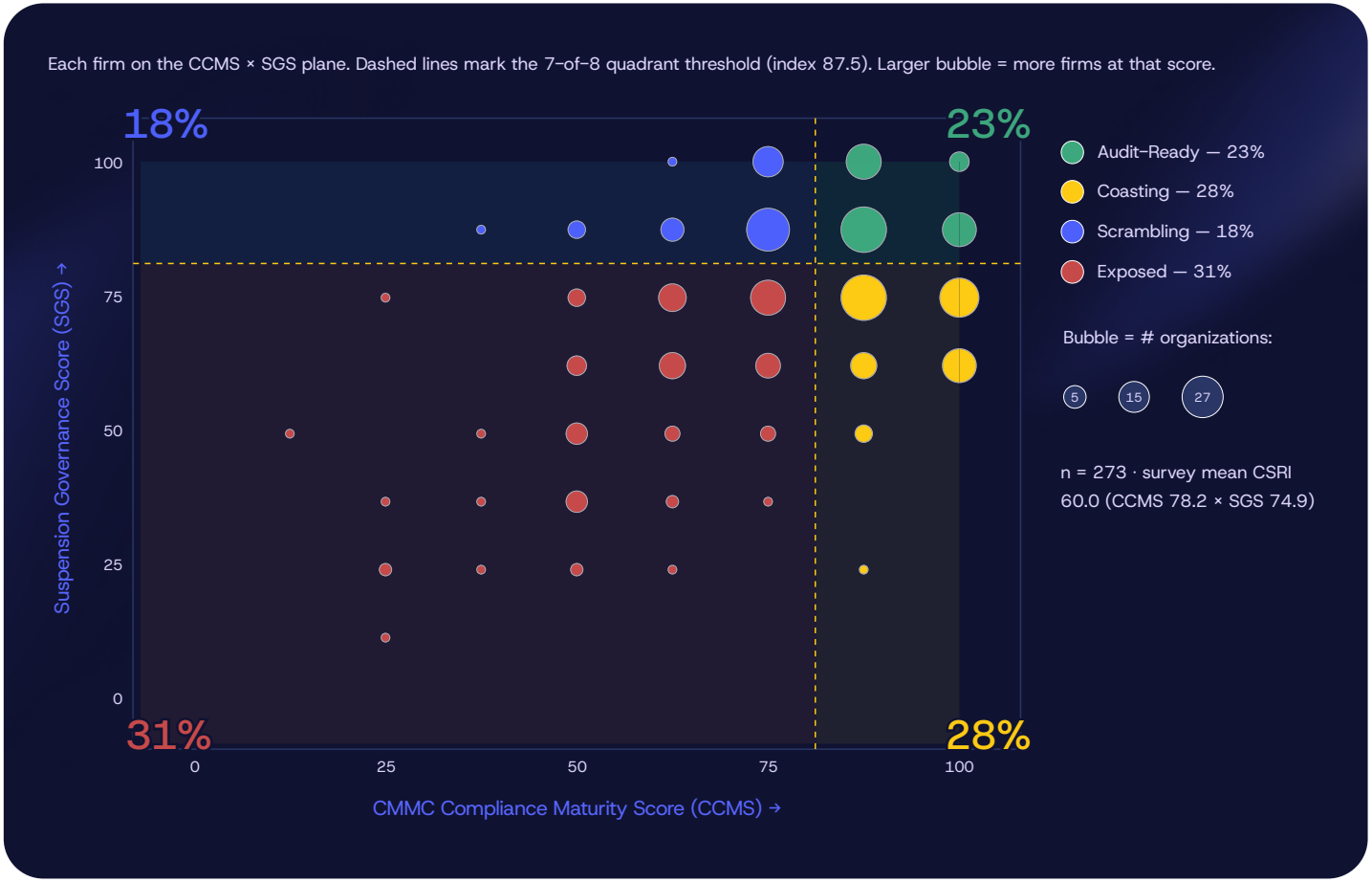
Indicator	% of respondents
s1 — Continued implementing technical controls as planned	62%
s2 — Budget not decreased or paused since the suspension	88%
s3 — Internal priority maintained or increased	89%
s4 — Communicated with primes/subs about flow-down expectations	62%
s5 — Actively evaluating new compliance tools or platforms	51%
s6 — Plans to submit comments on DoW's RFI	93%
s7 — Has a specific 60–90 day action plan	99%
s8 — Strengthening self-attestation documentation	55%

How CCMS and SGS Interact

CCMS and SGS are complementary but distinct measurements. CCMS measures compliance state — the foundational facts an organization can point to today. SGS measures governance behavior — what an organization is actively doing about the suspension right now. An organization can carry a strong CCMS alongside a weak SGS, or the reverse. Mapping the two together produces four quadrants that are more diagnostic than either score alone.

Where you draw the line between "strong" and "weak" on each dimension matters. The obvious cutoff — the midpoint of the 0–100 scale, a score of 50 — is too low for this group. Every respondent is already a confirmed DoW contractor carrying a live CMMC requirement, so nearly all of them clear 50 on both scores; at that cutoff, 93% land in the same quadrant and the framework tells you nothing. Setting the bar higher fixes that: an organization has to meet 7 of the 8 indicators on a dimension — an index of 87.5 — to count as strong on it. That threshold splits the population into a genuine, near-even four-way distribution, which is what makes the quadrants diagnostic.

Where the DIB Lands Across Four Quadrants



The plot makes the four-way split concrete. Each bubble is a set of organizations sharing the same CCMS and SGS score, sized by how many. Two things stand out. The lower-left Exposed quadrant — weak on both dimensions — holds the single largest share of the population at 31%, and the mass of the distribution sits below and to the left of the two threshold lines rather than in the upper-right corner. **Only 2% of organizations reach the top-right corner where both scores are perfect.** This is an already-qualified, already-engaged population, and it still does not cluster where readiness would put it.

CCMS ↓ SGS →	Low SGS (below 87.5) Passive Governance	High SGS (87.5+) Active Governance
High CCMS (87.5+) Compliance Foundation Strong	**COASTING** **28%** Compliant on paper, passive since the suspension. The false-confidence risk.	**AUDIT-READY** **23%** Strong on both compliance and governance. The destination — only 2% hit a perfect 8 of 8.
Low CCMS (below 87.5) Compliance Foundation Weak	**EXPOSED** **31%** Weak on both at once. The largest quadrant — and the priority target for action.	**SCRAMBLING** **18%** Active now, but without the compliance foundation to back it up.

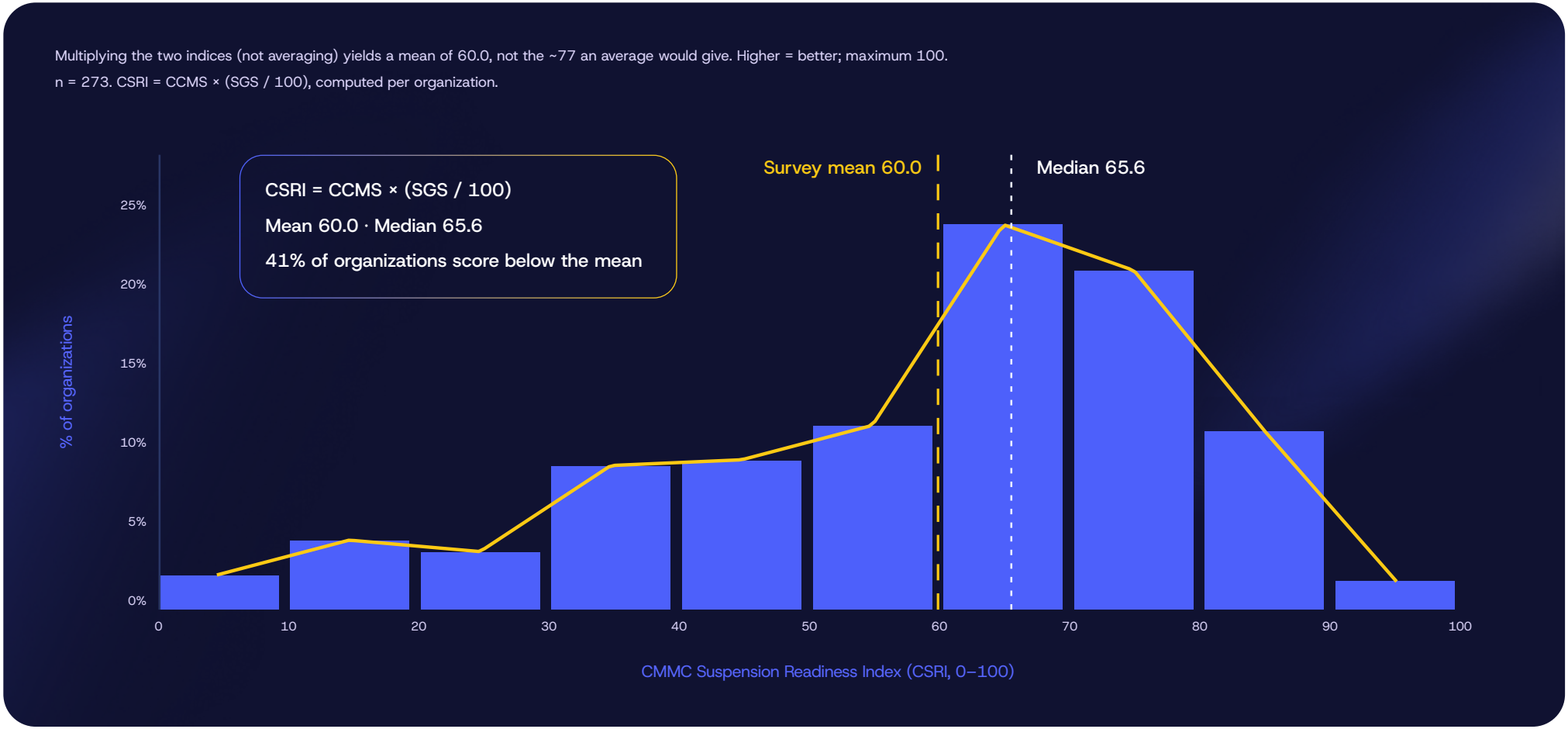
Quadrant thresholds (CCMS ≥87.5, SGS ≥87.5) are independent analytical cutoffs used in this diagnostic framework, calibrated to the 7-of-8 tier boundary described above rather than to a generic midpoint.

CMMC Suspension Readiness Index (CSRI)

CSRI = CCMS × (SGS / 100)

The formula multiplies by design: it takes an organization's compliance state and scales it by how much active governance stands behind it. At the survey means, averaging the two would produce a reassuring 77. Multiplying produces 60.0 — and that 17-point gap is the finding, not a quirk of the math. Averaging would let a strong compliance record paper over a passive response, and let a flurry of activity stand in for a weak foundation. Multiplication allows neither: a low score on either dimension pulls the whole result down. Readiness here is not two halves an organization can trade against each other; it is the product of both. A firm strong on one dimension and weak on the other is not comfortably in the middle — it is exposed on the side it neglected.

CSRI Distribution Behind the 60.0 Mean



The distribution is left-skewed, and the skew is the point. The median organization scores 65.6, but a heavy tail of low-scoring organizations — the Exposed quadrant mapped on the previous page — pulls the mean down to 60.0. 41% of organizations fall below the mean and 29% score below 50 on the 0–100 scale. Multiplication produces that shape: because a weak score on either dimension caps the combined result, the low tail fills out and the mean settles well below the median. Averaging the two indices would have reported roughly 77 and erased the tail entirely.

CCMS and SGS Quadrant Score Distribution

Tier	Indicators met	CCMS (% of respondents)	SGS (% of respondents)
Tier 1 — Nascent	0–4 of 8	14%	14%
Tier 2 — Developing	5–6 of 8	36%	45%
Tier 3 — Established	7 of 8	31%	29%
Tier 4 — Leading	8 of 8	20%	12%

Each dimension is tiered on its own 0–8 raw scale. CSRI itself is reported as a continuous 0–100 index rather than tiered, since it is the product of two already-tiered dimensions. Survey mean CSRI: 60.0 / 100. Median: 65.6 — higher than the mean, meaning this population clusters toward the high end with a smaller group of laggards pulling the average down. That is the opposite skew from Kiteworks' broader, unfiltered cross-industry survey research, where the equivalent combined index skews low with a long tail of high performers — a difference attributable to this survey's population, which pre-filters to organizations already confirmed to do business with the DoW and already carrying a live CMMC requirement, not to a different underlying phenomenon.

CSRI by CMMC Level

Level	CSRI Score
Level 3 (Expert)	62
Level 2 (Advanced)	56

Level 2 scoring lower than Level 3 is worth naming rather than smoothing over: it does not fit a simple "harder requirement, lower score" story, since Level 3 is the higher bar and scores above it. The roughly 7-point gap is large enough to be more than sampling variation, and it appears on both underlying dimensions, not just one. This report does not offer a cause for it — the survey was not designed to isolate one, and a confident explanation here would be speculation rather than a finding. It is flagged as the clearest open question for a follow-up wave. Level 1 (n=5) is excluded from this cut — too small to report.

CSRI by Industry

Industry	CSRI Score
Aerospace & Defense Manufacturing	66
Information Technology & Cloud Services	62
Telecommunications & Critical Infrastructure	59
Other Industries	52

Aerospace & Defense Manufacturing leads on CSRI, consistent with the segment's insulated bid-outcome profile described in the Market Consequences section. The Other Industries bucket trails — expected, given it aggregates six industries individually too small to report on their own, several of which (General Manufacturing, Higher Education) showed distinct, if directional-only, patterns earlier in this survey's analysis.

Action, Not Pause

Preparedness Didn't Pause

KEY FINDING

98% of respondents took at least one concrete action in response to the July 13 suspension. Only 2% did nothing — and budget reallocation moved toward compliance infrastructure, not away from it.

The suspension paused third-party assessment — not the Defense Industrial Base. The breakdown below shows what contractors did instead of waiting.

Actions Taken Since July 13, Full Distribution
(multi-select)

Indicator	% of respondents
Continued implementing technical controls as planned	62%
Communicated with primes/subs about flow-down expectations	62%
Began evaluating new compliance tools or platforms	51%
Reallocated CMMC-related budget to other priorities	49%
Paused or slowed vendor/tooling evaluations	32%
Taken no action either way	2%
Don't know	<1%

The budget reallocation is worth reading closely before it gets misread as retrenchment. 49% of respondents reallocated CMMC-related budget; however, reallocated does reallocated does not mean redirected away from compliance. Asked where that money went, 63% point to independently audited platforms such as FedRAMP-authorized tools, 55% to expanded audit logging and evidence-generation capability, and 49% to legal or compliance staff. Only 4% say no reallocation happened at all, and only 24% moved budget to cybersecurity priorities outside CMMC entirely. The reallocation is lateral, from one form of compliance spend to another, not an exit from compliance spend.

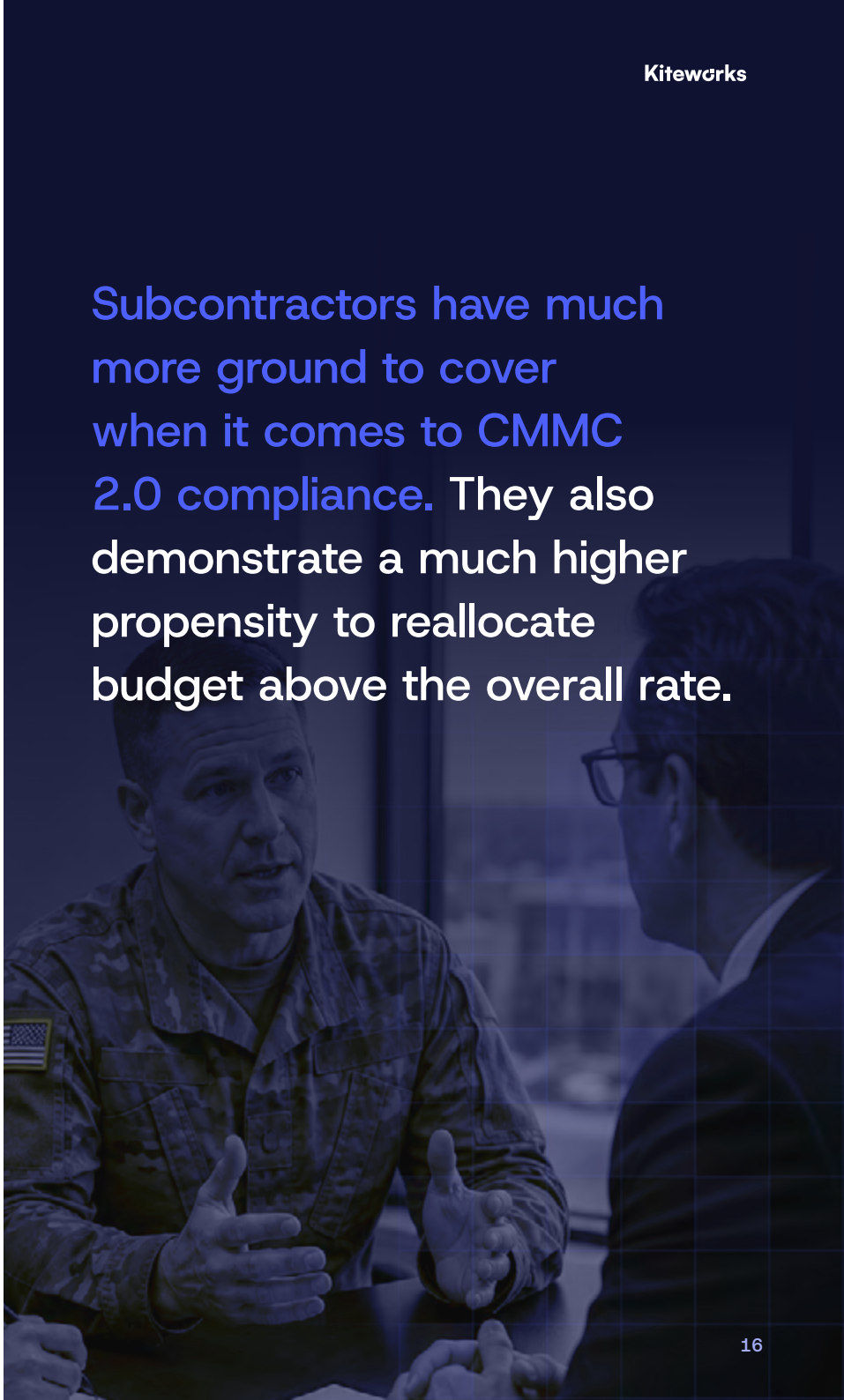
Where Reallocated Budget Went
(multi-select)

Answer Options	% of respondents
Independently audited platforms (e.g., FedRAMP-authorized tools)	63%
General business operations outside of security	57%
Expanded audit logging/evidence-generation capabilities	55%
Legal/compliance staff or outside counsel	49%
Other cybersecurity priorities outside CMMC	24%
Not applicable — no budget reallocation	4%

Segment cuts sharpen the picture further. Enterprises of 5,000 or more employees communicate with primes and subs about flow-down at less than half the overall rate — 36% versus 62% overall, the single largest gap in this entire question block. That could read as disengagement, but it more plausibly reflects standing channels: the largest organizations, disproportionately primes themselves, already have established flow-down relationships and may simply have less new ground to cover. It is worth a direct follow-up question in a future wave rather than assumed either way.

Tier 2-or-lower subcontractors reallocate budget above the overall rate — 63% versus 49% — and when they do, they redirect it toward independently audited platforms at the highest rate of any DIB-role segment: 82%, against 63% overall and just 56% among prime contractors. This is the same segment that, as the Market Consequences section documents, loses bids to Level 2 requirements at nearly double the overall rate. The smallest, least-leveraged part of the supply chain is investing hardest in the exact category of tooling this report finds the DIB values most.

Subcontractors have much more ground to cover when it comes to CMMC 2.0 compliance. They also demonstrate a much higher propensity to reallocate budget above the overall rate.



Legal and Regulatory Exposure

KEY FINDING

84% of respondents are concerned about False Claims Act exposure from an inaccurate self-attested SPRS score. RED FLAG: 80% of the 30 organizations in the survey's weakest compliance tier are still confident, very or somewhat, that their SPRS score would hold up under scrutiny (n=30). CCMS and SGS scores indicate otherwise.

The suspension paused verification. It did not pause the law. DFARS clause 252.204-7012 has required contractors handling covered defense information to implement NIST SP 800-171 controls and self-report their compliance status in the Supplier Performance Risk System since long before CMMC existed. Phase II was the independent-verification layer sitting on top of that obligation. Removing the verification layer does not remove the obligation — it removes the check on whether a contractor's own claim about its compliance is true.

That concern tracks a real, well-understood distinction: 73% of respondents say they are fully aware that DFARS 252.204-7012 remains a binding, standing obligation independent of CMMC Phase II, and a further 23% are aware but unsure of the full scope. Only 3% report no awareness of the distinction at all.

Logzone Check – The Enforcement Precedent That Makes This Concrete

On June 18, 2026, the Department of Justice announced a $507,144 False Claims Act settlement with LOGZONE Inc., a Huntsville, Alabama defense logistics contractor, over two U.S. Navy contracts. In October 2021, LOGZONE self-attested a perfect SPRS score of 110. When the Defense Contract Management Agency's DIBCAC unit independently assessed LOGZONE's actual NIST SP 800-171 implementation in February 2024, the real score came back at -170, near the bottom of the -203-to-110 possible range. DOJ alleged the company knowingly submitted invoices while its cybersecurity posture did not match what it had certified. Two features of the case apply to every respondent in

86% of organizations are concerned about flow-down obligations — prime-to-sub CMMC requirements.

92% of organizations have engaged some form of legal review related to False Claims Act exposure.

this survey, not just to defense-logistics contractors: it was not whistleblower-driven — DOJ built it from a routine DIBCAC audit, the same kind of government-led review this survey confirms remains active during the suspension — and the gap that mattered was severe, not a good-faith control-by-control disagreement. With Phase II's third-party check suspended, government audits and prime due-diligence reviews are, for most of the DIB, the only mechanism standing between a self-attested score and an FCA referral.

Confidence pulls away from actual compliance even more sharply here than the cascade in the Executive Summary already showed. Among the 30 respondents whose current self-assessment status is partially compliant, not started, or still in early stages — the weakest tier this survey measures — 80% are nonetheless confident, very or somewhat, that their SPRS score would hold up if reviewed today. However, confidence is not tracking the underlying compliance state here. It is detached from it.

The DIB has not been idle on the legal side. 92% of respondents have engaged some form of legal review specifically to assess False Claims Act exposure since the suspension: 43% brought in outside counsel, 49% ran an internal legal or compliance review. But the pattern among the remainder is telling. Of the 15 respondents who have not yet engaged any review but plan to, only 33% describe themselves as "very confident" in their SPRS score — at the 50% sample-wide rate or below — and 27% say they are "not very confident," against 4% overall. Legal review in this survey looks reactive, not routine: the respondents seeking it are already the least confident, not the most diligent.

Asked what would most increase confidence that a self-attested score could withstand scrutiny, respondents point to evidence, not paperwork: 47% cite a complete, real-time audit trail of system and data access activity, and 36% cite independent third-party authorization of the platforms underlying their compliance posture, such as FedRAMP. Only 11% point to a dedicated legal or compliance review of the attestation itself. The DIB's own instinct is that a self-attestation is only as defensible as the evidence behind it — not the legal opinion defending it.

Flow-down risk concentrates where contractual privity is weakest. 86% of respondents are concerned about flow-down obligations — prime-to-sub CMMC requirements — continuing unchanged despite the suspension. That concern is not evenly spread: it is highest among Tier 1 subcontractors (92%) and Tier 2-or-lower subcontractors (89%), and lowest among prime contractors (79%), with organizations that are both a prime and a subcontractor in between (89%). A prime that certifies compliance to the government while relying on a subcontractor's

unverified self-attestation inherits that subcontractor's risk, and a subcontractor without a direct government relationship has less visibility into how its own attestation gets used upstream. The anxiety concentrates exactly where that structural exposure is greatest.

External Validation — This Isn't a DIB-Specific Anxiety

Breaches that involve a third party grew 60% year-over-year and now account for 48% of all breaches studied, according to the Verizon "2026 Data Breach Investigations Report."[8] That makes the flow-down risk this survey measures an industry-wide trend, not a CMMC-specific one. In the Public Administration sector specifically, a third party was present in 36% of breaches, and the human element (error or misuse) was present in 69% — the same categories (documentation gaps, misdelivery, privilege misuse) this report's confidence-evidence gap describes.

Separately, the IBM "Cost of a Data Breach Report 2026: The AI Tipping Point" found supply chain compromise was the single costliest factor of 30 studied for increasing breach cost — adding USD 227,250 above the USD 4.99 million global average — and that noncompliance with regulations added a further USD 201,112.[9] Getting the self-attestation right is not only a legal question; it is a quantifiable cost question.

The World Economic Forum's "Global Cybersecurity Outlook 2026" reports that 65% of large organizations now rank third-party and supply-chain vulnerabilities as their single greatest challenge to cyber resilience, up from 54% the prior year.[10] Concern without visibility is the same gap this report finds between SPRS confidence and current, evidence-backed submissions.

KEY FINDING

Tier 2-or-lower subcontractors lose or are disqualified from bids at 55% — nearly double the 31% rate among prime contractors. The suspension opened a door for some bidders and closed one for others, in the same population, at the same time.

Market Consequences Are Already Visible

55% of respondents are now bidding on solicitations they would previously have avoided over Level 2 requirements. The suspension removed a barrier to entry for some. But 52% also report withdrawing from a bid rather than pursue certification, and 38% report losing or being disqualified from a contract because of the same requirement. Both effects are live in the same population.

Bid Outcomes Tied to Level 2 Requirements

Indicator	% of respondents
Won a contract after achieving or attesting Level 2 readiness	59%
Withdrew from a bid rather than pursue Level 2 certification	52%
Lost or was disqualified from a contract due to Level 2 requirements	38%
Delayed a bid decision pending Level 2 clarity	37%
None of the above	6%

Which side of the ledger an organization lands on tracks its position in the supply chain more than its posture toward the suspension. Tier 2–or–lower subcontractors lose or get disqualified from bids at 55% — nearly double the 31% rate among prime contractors, and well above the 38% overall rate. Organizations that are both a prime and a subcontractor sit in between at 43%. Bid loss concentrates in exactly the segment with the least leverage to negotiate around a Level 2 requirement.

Aerospace & Defense Manufacturing is the most insulated industry in this survey. 16% report a loss or disqualification, against 38% overall, and 36% report a bid withdrawal, against 52% overall — still the lowest of any industry, consistent with the segment's highest CSRI score in this report's readiness framework.

A consistency check on the "bidding plans unchanged" segment (10% of the sample): this group does not show an elevated delayed-bid rate in this data pull — 39%, close to the 37% overall rate, versus a meaningful gap in an earlier data pull. The prior claim that this group faced a distinct "waiting on clarity" pattern does not hold up here and has been dropped rather than carried forward on the strength of a smaller, earlier sample.

Assessor and Platform Priorities

KEY FINDING

89% of respondents are already using, or plan to adopt within six months, an independently audited platform such as a FedRAMP-authorized tool. The DIB is not waiting for the Reform Task Force to decide before it invests.

93% say third-party authorization will be essential or important to future vendor selection. This section covers what the DIB is looking for in that tooling, and separately, what it is looking for in the assessor relationship.

Vendor Evaluation Capabilities That Matter Most
(select up to three)

Indicator	% of Respondents
Independent third-party authorization (e.g., FedRAMP)	51%
Built-in NIST SP 800-171 / CMMC 2.0 control support out-of-box	48%
Ease of integration with existing systems	47%
Vendor's track record with DoW / DIB customers	44%
Real-time audit logging and evidence generation	40%
Cost / total cost of ownership	37%
Single-tenant or sovereign deployment options	28%

Secure Data Exchange Capabilities That Matter Most
(select up to three)

Indicator	% of Respondents
Automated DLP / content inspection on outbound CUI	52%
Encrypted managed file transfer (MFT) for CUI exchange	50%
Integration with existing collaboration tools	49%
Centralized audit logging of external data-exchange activity	41%
Secure email encryption and policy enforcement	40%
Granular, role-based access controls for external recipients	35%
None of the above / not a priority	1%

Encrypted MFT moved above collaboration-tool integration in this data pull (50% vs. 49%, a near-tie that swapped rank order from an earlier pull) — worth noting as a rank change, not a substantive shift, since the two rates sit within a point of each other.

Where the DIB Turns for CMMC Guidance
(multi-select)

Indicator	% of Respondents
Technology / platform vendor guidance	63%
Direct federal guidance (DoW, SAM.gov)	53%
C3PAO or independent compliance consultant	48%
Internal legal / compliance team	37%
Industry association or trade group	34%
Outside counsel (government contracts)	32%
Prime contractor guidance	31%

Technology and platform vendors (63%) are the most-relied-on source of CMMC guidance, ahead of direct federal guidance (53%) and independent assessors (48%) — vendors, the government, and C3PAOs are the DIB's top three channels, in that order.

A C3PAO or independent compliance consultant is the third most-relied-on guidance source in this survey — ahead of internal legal/compliance, trade associations, outside counsel, and prime guidance. That reliance holds even without a mandate forcing it: 96% of respondents have engaged a C3PAO for Level 2-or-above assessment at some point, and 32% are continuing a scheduled assessment voluntarily, for internal assurance, with no deadline compelling them to. 93% plan to submit comments on DoW's Request for Information on recognizing commercial tools in a future CMMC framework, either directly (63%) or through an industry association (31%).

Read together, the platform and assessor findings point in the same direction without competing for the same budget line: the DIB wants independently audited, evidence-generating technology to support its self-attestation, and it wants an independent assessor relationship to validate the underlying compliance posture the technology documents. Neither substitutes for the other in this survey's own data.

The Human Element: Knowledge Gaps and the Confidence Illusion

Only 3% of respondents believe every CMMC-related requirement is currently paused. On the surface, that reads as reassurance: 97% of the DIB correctly knows something survived the suspension. Ask which specific obligations, and the picture changes.

What Respondents Understand Remains In Effect
(select up to three)

Areas of Impact	% of respondents
DFARS clause 252.204-7012 remains binding	80%
NIST SP 800-171's 110 controls remain in effect	67%
Phase 1 self-assessment requirements remain in effect	52%
Select government-led assessments remain in effect	43%
None of the above — believe all requirements are paused	3%
Don't know	3%

48% of the DIB does not know that Phase 1 self-assessment obligations continue,[11] and 57% do not know that select government-led assessments continue. Self-attestation accuracy is exactly where False Claims Act exposure concentrates, which makes the Phase 1 gap the more consequential of the two.

Self-reported confidence barely tracks this knowledge. Scored against the four factual items (excluding the misconception and "don't know" options), the average respondent gets 2.42 of 4 correct. Respondents who call themselves "very confident" in their understanding average 2.48 — statistically indistinguishable from the 2.48 average among respondents who call themselves only "somewhat confident." The two largest confidence tiers in this survey know almost exactly the same amount.

KEY FINDING

49% of respondents who call themselves "very confident" in their understanding of the suspension scored below 3 of 4 on a direct knowledge test. Confidence in this survey does not track knowledge — it tracks something else.

Knowledge Score (0–4 Correct) By Self-Reported Confidence

Mean Knowledge Score	Mean score (out of 4)
"Very confident" respondents	2.48 / 4
"Somewhat confident" respondents	2.48 / 4
"Not very confident" respondents	1.43 / 4
"Not at all confident" respondents	0.67 / 4

Each respondent answered four factual questions about what the July 13 suspension did and did not change. The score is the number correct, out of four.

Both directions of miscalibration are real, not just one. 49% of "very confident" respondents scored below 3 of 4 — nearly half, genuinely overconfident. 56% of "somewhat confident" respondents scored 3 or better — meaningfully underconfident relative to what they know. This survey's confidence question is not measuring knowledge. It is measuring something else, weakly related to whether the respondent can correctly name what the suspension did and did not pause.
17% of the full sample scored a perfect 4 of 4; 5% scored zero.

Where an organization learned about the suspension shapes how well it understood it. Respondents who learned via direct DoW or government communication (44% of the sample, the largest single channel) report the highest "very confident" rate: 63%, above the 57% overall average. Respondents who learned via an industry association or trade group report the lowest: 38%, a meaningful gap even at this small n. Trade associations exist partly to translate policy for their members; on this data, their members understand the change worse than those who went to the primary source. The channel's sample is small (n=13) but the direction is consistent with an earlier data pull.

Poor knowledge does not automatically mean low concern, but it does not guarantee appropriate concern either. Among the 55 respondents who scored 0 or 1 of 4 on the knowledge questions, 69% are still "very" or "somewhat" concerned about False Claims Act exposure — roughly proportional to the sample overall. But a combined 31% of this same poorly-informed group are "not very" or "not at all" concerned. That pocket, uninformed and unworried at the same time, is the genuine blind spot this section identifies — not the population that knows little and is anxious about it, which is at least a coherent, self-correcting state.

Cross-Analyses: Variations by Key Factors

Two kinds of variation matter here. The first is variation by who an organization is — its industry, size, supply-chain position, and region. The second, and the more revealing, is variation by what else an organization said: how one answer moves with another. The demographic cuts describe where readiness sits. The answer-to-answer relationships describe why it sits there.

What the Answers Reveal About Each Other

The most counterintuitive relationship in this survey is between understanding and worry. Organizations that describe themselves as fully confident in their understanding of what the suspension changed are the most concerned about False Claims Act exposure, not the least: 57% of them are "very concerned," against 40% of the sample overall. Organizations only "somewhat confident" in their understanding are the least concerned, at 20%. The same pattern holds on awareness of DFARS 252.204-7012 as a standing obligation: organizations fully aware of it are "very concerned" about FCA exposure at 47%, against 23% among those aware but unsure of its scope. Understanding the suspension does not calm legal concern. It sharpens it — because the concern is the correct response to an accurate picture. Education that closes the knowledge gap this report documents will not reduce anxiety in the DIB. It will increase it, appropriately.

The confidence-evidence gap has a legal-review shape as well. Organizations that have engaged outside counsel are the most confident in their SPRS score (66% "very confident, fully evidence-backed"), while organizations that have not yet engaged any review but plan to are among the least confident (33% very confident, 27% "not very confident" — against 4% not-very-confident sample-wide). Legal review

in this survey is reactive, not routine: the organizations seeking it are the ones that already suspect a problem, not the ones being most diligent in advance. The direction of causation runs from concern to review, not from review to confidence.

What organizations want from a compliance platform depends sharply on how ready they already are. Among organizations already running a FedRAMP-authorized platform, 55% name independent third-party authorization as a top vendor-evaluation criterion. Among the genuine fence-sitters — organizations only "somewhat likely" to adopt such a platform — that figure collapses to 19%, while cost/total-cost-of-ownership (54%) and built-in out-of-box control support (65%) dominate. The organizations furthest from adoption are not weighing the FedRAMP credential at all; they are weighing price and setup effort.

Even the most confident organizations still want more independent validation, not less. Among organizations that call their SPRS score fully evidence-backed, 54% say independent third-party platform authorization would further increase their confidence — the single most-named answer for that group. Among the least-confident organizations, the top answer shifts to a dedicated legal review (45%). The confident want stronger technical evidence; the unconfident want a legal opinion first. Both are asking for something outside their own attestation to stand behind it.

Two patterns in the data reinforce each other — a sign the responses hang together — and together they isolate the organizations that genuinely stepped back. Budget and priority move in lockstep: among organizations that paused their CMMC budget entirely pending the review, 92% now report a lower or shelved priority

54% vs. 45%

Even organizations that call their SPRS score fully evidence-backed still want more validation, not less: 54% say independent platform authorization would increase their confidence further. Least-confident organizations shift to wanting a legal review first (45%).

and none report a higher one, while among organizations that made no budget change, 33% report a higher priority and just 6% a lower or shelved one. The roughly one in eight organizations that truly pulled back are visible in both measures at once — a small, coherent minority, and the clear exception to the majority that kept their CMMC programs moving, as the Key Findings describe. "Paused" itself is not a single condition. The two paths to a stalled C3PAO assessment look very different: organizations whose assessment was cancelled by the assessor report the survey's highest SPRS-submission currency (85%), while those that never scheduled one sit at 43% and those that never engaged a C3PAO at all sit at 10%. A paused assessment can mean at least three different things, each with very different readiness behind it.

Industry Variations

Aerospace & Defense Manufacturing leads the CSRI distribution at 66.2, followed by Information Technology & Cloud Services at 61.9, and Telecommunications & Critical Infrastructure at 59.3. The combined Other Industries bucket trails at 52.2. Telecom/Critical Infrastructure's behavioral profile earlier in this report — voluntarily pausing scheduled C3PAO assessments at nearly double the overall rate rather than treating them as cancelled, while showing the lowest SPRS submission currency of any industry — reads as an industry proceeding cautiously rather than one that has either fully stopped or fully finished.

DIB Role Variations

CSRI By DIB Role

DIB Type	CSRI Score
Both a prime and a subcontractor	64.7
Prime contractor	61.6
Subcontractor (Tier 1)	52.1
Subcontractor (Tier 2 or lower)	52.2

Regional Variations

North America (United States and Canada, 60% of the sample) posts a mean CSRI of 64.7. Europe (France, Italy, Netherlands, United Kingdom, Germany, and Belgium combined, 38% of the sample) posts 53.9 — an 11-point gap. Within Europe specifically, France and the Netherlands show different profiles on individual measures: France (n=58) reports one of the lowest SPRS submission rates in the survey (43%) alongside the highest FCA concern (88%), while the Netherlands (n=22) shows a similar submission rate (50%) with comparably high concern (86%) — a mismatch between exposure and awareness that may be the more urgent gap of the two, since concern is what tends to precede action elsewhere in this data.

The gap is not only in the composite score. Europe is the most exposed regional segment on every readiness measure. 44% of European organizations fall in the Exposed quadrant — weak on both compliance maturity and suspension governance — against 21% in North America and 31% across the full sample, while only 15% reach Audit-Ready versus 23% overall. Current self-attestation is where the divergence is sharpest: 43% of European organizations hold a current SPRS submission, against 70% in North America and 59% across the full sample — the least-current self-attestations of any region. Confidence does not track that evidence. 94% of European respondents remain confident their self-attested score would hold up under review, almost identical to North America's 96%. European suppliers inside U.S. Department of War supply chains inherit the same CMMC obligations by flow-down, and face them from a measurably weaker posture.

Organization Size Variations

CSRI By Organization Size

Employee Numbers	CSRI Score
5,000 or more employees	**57.8**
1,000 to 4,999 employees	**64.2**
500 to 999 employees	**58.7**
250 to 499 employees	**54.3**
50 to 249 employees	**51.9**

CSRI is not strictly monotonic with size. The largest organizations (5,000+) score below the two mid-size tiers, not above them — consistent with this report's earlier finding that the largest enterprises communicate with primes/subs about flow-down at far below the overall rate, which drags down their SGS component even where their underlying compliance state (CCMS) is strong. The smallest organizations (50–249 employees) score lowest overall, consistent with the under-resourced-not-unconcerned profile described earlier: lower budget tiers, lower near-term FedRAMP adoption intent, and lower DFARS 7012 awareness, but no evidence of deliberate deprioritization.

Three-Way Interaction: CMMC Level × DIB Role × Actions Taken

Crossing CMMC level and DIB role together against the continuity measures surfaces one combination that breaks from every other cell tested. Level 3-required Tier 1 subcontractors (n=20) fall well below the overall rates on both continuity measures: 35% continued technical controls as planned and 45% communicated with primes and subs about flow-down, against 62% overall on each. Every other level-by-role combination in this survey lands closer to both overall rates. This sharpens the standalone Tier 1 finding elsewhere in this report. On overall CSRI, Tier 1 and Tier 2-or-lower subcontractors are indistinguishable (52.1 vs. 52.2); the weak spot is not Tier 1 subcontractors broadly but specifically Tier 1 subcontractors facing the highest compliance bar, the combination of least leverage in the supply chain and the steepest requirement at once. The sample is small and this should be read as the sharpest hypothesis in this report for a follow-up wave, not a settled finding.

Implications and Recommendations

Business and Strategic Implications

The suspension changed who verifies compliance, not what compliance requires. DFARS 252.204-7012 and the underlying NIST SP 800-171 obligation did not pause, **and neither did the DOJ's Civil Cyber-Fraud Initiative, the enforcement mechanism behind the LOGZONE settlement this report describes.** An organization that treats the Phase II suspension 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 specifically: the 31% of this survey's population scoring low on both CCMS and SGS at once is not a fringe segment. It is more than a quarter of a population already qualified to do DoW business and already carrying a live CMMC requirement. Budget conversations framed around "waiting to see how the Reform Task Force review concludes" should be weighed against this report's confidence-evidence gap finding — only 60% of organizations that call themselves confident in their SPRS score have a submission that is in fact current, and a legal exposure that predates the suspension does not wait for a policy review to conclude.

Operational Recommendations

The platform track

The single weakest CCMS indicator in this survey is FedRAMP-authorized platform adoption, at 35%. The single weakest SGS indicator is active evaluation of new compliance tooling, at 51%. Both are directly addressable through vendor evaluation and procurement — not through waiting on the Reform Task Force. Organizations should prioritize independently audited, evidence-generating secure data exchange capable of producing the audit trail 47% of respondents already say would most increase their own confidence in their self-attestation.

The independent-assessment track

96% of this survey's respondents have already engaged a C3PAO, and 32% are continuing a scheduled assessment voluntarily, with no deadline compelling them to do so. Organizations sitting on a paused or cancelled assessment should treat voluntary continuation as the default, not the exception this survey shows it already is for nearly a third of the DIB. An independent third-party assessment produces exactly the validation the confidence-evidence gap shows self-attestation alone cannot — the check the suspension removed, not the obligation it left standing.

CMMC Readiness Checklist

The 16 indicators behind this report's CCMS and SGS scores, restated as a self-scoring checklist. Score one point for every box checked; 7 or more on either dimension places an organization in this report's Tier 3 (Established) or higher.

Compliance Maturity (CCMS)

- ☐ Self-assessment is substantially or fully compliant and documented
- ☐ SPRS score is submitted and current
- ☐ A C3PAO has been engaged for Level 2+ assessment
- ☐ Fully aware DFARS 252.204-7012 shapes compliance strategy
- ☐ No belief that all CMMC requirements are currently paused
- ☐ Meaningful budget committed, $150,000 or more
- ☐ Legal/compliance review conducted since the suspension
- ☐ Already using a FedRAMP-authorized platform

Suspension Governance (SGS)

- ☐ Continued implementing technical controls as planned
- ☐ Budget has not been decreased or paused since the suspension
- ☐ Internal priority maintained or increased
- ☐ Communicated with primes/subs about flow-down expectations
- ☐ Actively evaluating new compliance tools or platforms
- ☐ Plans to submit comments on DoW's RFI
- ☐ Has a specific 60–90 day action plan
- ☐ Actively strengthening self-attestation documentation

Multiply your two box counts to estimate a CSRI: (CCMS boxes checked ÷ 8) × (SGS boxes checked ÷ 8) × 100 to estimate a CSRI. A score in this report's Exposed quadrant — below 7 on both dimensions — describes 31% of this survey's population and is the profile most exposed to the legal and market consequences this report documents.

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 help shape what CMMC becomes next. That is the headline — and it is arithmetic, not optimism.

It is also not the whole story. More than a quarter of this already-qualified, already-engaged population scores low on both compliance state and active governance at once, and the confidence-evidence gap that defines this report runs straight through it. The suspension removed the third-party check on self-attestation. It did not remove the obligation the check was there to verify — and recent Department of Justice enforcement has shown that an inaccurate score does not need a whistleblower to surface. A routine government audit is enough.

That is why the pause is a window, not a reprieve. This report's CCMS, SGS, and CSRI framework sets a 2026 baseline; a future wave will show whether the gap it documents narrows or widens. The organizations that use the pause to turn confidence into evidence will be the ones ready when the assessor returns. The rest will still be Exposed when it does.

96% are confident their self-attested SPRS score would hold up. Under 30% can prove it.

Legal Disclaimer

The information provided in this report is for general informational purposes only and should not be construed as professional, legal, or compliance advice. Kiteworks, and any other contributing organizations make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained in this report. Any reliance placed on this information is strictly at the reader's own risk. Readers should consult qualified legal counsel and cybersecurity professionals when addressing specific compliance requirements.

Regulatory-staleness note: this report describes the state of CMMC 2.0 Phase II, the associated Reform Task Force review, and related DFARS/FCA enforcement activity as of July 29, 2026. All regulatory and legal claims in this report were verified against dated sources as of that date (see Endnotes) and are recency-sensitive — readers should confirm current status before relying on any regulatory claim in this report, particularly given the Reform Task Force's report was expected by mid-September 2026, after this report's fielding and drafting window.

Endnotes

1. U.S. Department of War, suspension of CMMC 2.0 Phase II third-party assessments, July 13, 2026. Justin Doubleday, "Pentagon suspends CMMC Phase Two requirements, launches review of program," Federal News Network, July 13, 2026, https://federalnewsnetwork.com/cybersecurity/2026/07/pentagon-suspends-cmmc-phase-two-requirements-launches-review-of-program/; U.S. SBA Office of Advocacy, July 20, 2026.
2. DFARS clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," U.S. DoD, https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting; Crowell & Moring LLP.
3. Self-attested SPRS scores carry False Claims Act exposure risk absent third-party assessment; U.S. DOJ Civil Cyber-Fraud Initiative. Foley & Lardner LLP, "DOJ's LOGZONE Settlement Highlights FCA Risk in Cybersecurity Compliance Representations," July 2026, https://www.foley.com/insights/publications/2026/07/dojs-logzone-settlement-highlights-fca-risk-in-cybersecurity-compliance-representations/.
4. U.S. DOJ, Office of Public Affairs, "Alabama Defense Contractor Agrees to Pay $507,144 to Resolve False Claims Act Liability Relating to Cybersecurity Violations," June 18, 2026, https://www.justice.gov/opa/pr/alabama-defense-contractor-agrees-pay-507144-resolve-false-claims-act-liability-relating.
5. Kiteworks, "State of CMMC 2.0 Preparedness in the DIB," March 26, 2025, https://www.kiteworks.com/cmmc-preparedness-dib-report/.
6. U.S. DoW, CMMC Reform Task Force Request for Information (comments due 12:00 p.m. ET, August 14, 2026). U.S. SBA Office of Advocacy, July 20, 2026, https://advocacy.sba.gov/2026/07/20/dow-requests-information-for-cmmc-reform-task-force/.
7. CMMC Reform Task Force 60-day review, report expected mid-September 2026. WilmerHale, July 20, 2026, https://www.wilmerhale.com/en/insights/client-alerts/20260720-pentagon-suspends-cmmc-phase-2-requirements-and-launches-review-of-cybersecurity-certification-program.
8. Verizon Business, "2026 Data Breach Investigations Report," 2026, https://www.verizon.com/business/resources/reports/dbir/.
9. IBM Security, "Cost of a Data Breach Report 2026: The AI Tipping Point," Ponemon Institute, 2026, https://www.ibm.com/reports/data-breach.
10. World Economic Forum, "Global Cybersecurity Outlook 2026," January 2026, https://www.weforum.org/publications/global-cybersecurity-outlook-2026/.
11. Phase 1 self-assessment requirements remain in effect. Morgan Lewis, July 2026, https://www.morganlewis.com/pubs/2026/07/department-of-war-suspends-cmmc-phase-ii-requirements-but-cybersecurity-obligations-remain.

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.

August 2026

www.kiteworks.com