The November Wall

An opinion on what is actually happening in the defense industrial base — and why the next 28 months will re-price it.

The views below are the author's. Every factual claim is sourced in the endnotes. July 2026.

The wall is real, and the math does not close

On November 10, 2026, third-party CMMC Level 2 certification becomes a condition of award for Department of Defense contracts involving controlled unclassified information. That is Phase 2 of the rule that took effect last November, and as of this writing no delay has been announced.[1][2]

Here is the arithmetic the defense industrial base is quietly living with. DoD's own estimate is that roughly 80,000 companies will need Level 2 certification.[3] As of the Cyber AB's May town hall, 1,391 final Level 2 certificates had been issued — under 2% of the requirement — with about 100 authorized C3PAOs and fewer than 800 certified assessors to process the rest.[4][5] Assessment waits already run about six months and are projected to stretch past eighteen by fall.[6] Typical contractors need six to twelve months of remediation before they can even sit for an audit.[6]

Tens of thousands of companies need a certification that the assessment ecosystem cannot deliver on time. A large share of the defense industrial base is about to become contract-ineligible through no fault of its engineering or its order book. That sentence should be read twice.

The primes became the regulators

The most important enforcement of CMMC is not coming from the Pentagon. It is coming through supplier portals.

L3Harris Missile Solutions has told CUI-handling suppliers at every tier to show proof of Level 2 certification by July 30, 2026 — three and a half months before the government requires it — or be "precluded from the program."[7] Elbit America went from a polite November advisory to, by January, "suppliers failing CMMC flow-downs will not receive purchase orders," and by February was openly assembling a network of certified suppliers.[8] By late 2025, 47% of surveyed subcontractors had already received a CMMC flow-down request from a prime.[9]

This is rational behavior. The primes carry the flow-down risk, their programs depend on supplier survival, and they ended FY2025 with a combined $1.36 trillion of backlog to protect.[10] But it means the effective deadline for a Tier 2 or Tier 3 supplier is not November 10. It is whenever their prime's supplier-portal notice says it is — and for some, that date has already passed.

Meanwhile, the customer went AI-first

While its supply base wrestles with certification, the Department itself crossed an adoption threshold that most of the commercial economy has not.

The FY2026 budget reached $1 trillion, including the first dedicated AI and autonomy budget line at $13.4 billion.[11][12] In mid-2025 the CDAO handed frontier-AI agreements of up to $200 million each to OpenAI, Anthropic, Google, and xAI.[13] GenAI.mil launched in December and reached roughly 1.5 million users inside six months; ChatGPT — certified for CUI at Impact Level 5 — arrives for over 3 million defense personnel this month.[14][15] The Department's January AI strategy mandates that the latest frontier models be deployed within 30 days of public release.[16]

Read those two stories together and the asymmetry is stark: the customer is institutionalizing AI at a pace commercial enterprises would consider reckless, while telling its suppliers — in rule and in flow-down — that they may not touch controlled data with unmanaged tools. Suppliers are being simultaneously forced toward AI and forbidden from adopting it carelessly. The only way through that contradiction is compliant architecture: approved clouds, bounded data, auditable systems, and increasingly, models you own rather than rent. Even the government is hedging against model lock-in: the FY26 NDAA requires a department-wide AI model assessment framework, and commentators are already warning about "vendor lock" in the $1 deals.[17][18]

Capital has already noticed

Aerospace and defense deal value climbed from about $27 billion in 2024 to over $30 billion in 2025 and is tracking toward $32 billion this year, with PE-backed roll-ups of Tier 2/3 suppliers named explicitly as an active thesis.[10] Defense-tech venture funding hit $14.6 billion in the first five months of 2026 — already past 2025's full-year record.[19]

The detail that should stop a seller mid-sentence: certification now moves price. In the $10M–$50M enterprise-value band, machine shops with NADCAP, ITAR registration, and CMMC progress traded one and a half to two and a half EBITDA turns above otherwise identical peers over the past eighteen months.[20] Defense

electronics platforms command roughly 18.7x EV/EBITDA against about 15x for broader defense peers.[21] Compliance has become a valuation asset class. The buyers know it before the sellers do.

The exodus paradox

The forecast everyone quotes says 33,000 to 44,000 companies — 15 to 20 percent of the DIB — will exit rather than certify, most of them this year.[22] The canonical case is a $2 million machine shop staring at $200,000 of compliance cost to protect $400,000 of defense revenue. First-year compliance realistically runs $98,000 to $305,000, and assessment fees alone are climbing as demand outstrips the assessor supply.[23]

And yet: Elbit, having talked to more than a thousand of its suppliers, reports that fewer than one percent have said they are walking away.[24] Both things can be true. Companies with real defense revenue are finding paths — enclaves, managed environments, early certification. Companies for whom defense was marginal are quietly letting it go. That is not an exodus; it is a sorting. The suppliers that remain will be fewer, more certified, more valuable, and more acquirable.

What I think is actually happening

Put the four pieces together — a hard certification wall, primes enforcing it early, a customer institutionalizing AI, and capital paying certified premiums — and the picture is not a compliance story. It is a re-rating.

For a generation, small defense manufacturers traded at machine-shop multiples because they ran on tribal knowledge: excellent hands, hero effort, spreadsheets, and key-person risk everywhere a buyer looked. What CMMC did — accidentally — was force the entire base to put a price on operational discipline. What AI does is make that discipline compound: a company whose operations run on owned, auditable intelligence gets structurally better every quarter, and can prove it in diligence.

The winners of the next 28 months will be the companies that treat the wall as a forcing function: certify early, instrument the business, and build intelligence inside the compliance boundary they already paid for. They will be worth more, twice — once for the eligibility their certified status protects, and once for the operating system a buyer inherits. The losers will be excellent companies that waited, and will sell at distressed multiples for reasons unrelated to their fundamentals. Well-run businesses will trade cheap because of paperwork. That is a tragedy for sellers and the opportunity of a generation for consolidators.

What operators should do now

1. Baseline everything this quarter. Close cycle, on-time delivery, CTB hours, AP cost per invoice, win rate. Improvement you cannot prove is improvement a buyer will not pay for.
2. Treat certification as an asset purchase, not a tax. One to two and a half EBITDA turns of premium against a low-six-figure cost is the best capital allocation available to most owners in this market.[20][23]
3. Put AI inside the boundary, not around it. Approved cloud, documented CUI classification, written governance policy, audit trails. The policy alone changes adoption behavior.
4. Own your intelligence. Model-agnostic architecture and, where the economics justify it, models you control — the customer itself is being told to avoid single-model dependence.[17]
5. Decide your M&A posture on purpose. In a sorting market, you are consolidating or being consolidated; drifting is a decision too, just a bad one.

The honest caveat

Two things could soften this thesis. First, CMMC has slipped before — announced in 2019, torn up in 2021, rewritten since — and pressure for waivers, alternative pathways, or timeline relief will mount by Q4 as the capacity gap bites.[25] But betting your backlog on a delay is a poor trade when your primes are enforcing early regardless. Second, the AI half can be oversold: Gartner has generative AI in its trough of disillusionment, Deloitte finds defense factory-floor pilots hard to scale, and MIT's much-quoted study found 95% of enterprise GenAI pilots show no measurable P&L return.[26][27] The failures share a pattern, though: tools bolted on without governance, data discipline, or ownership. The prescription above is the treatment for exactly that disease.

The wall is four months away. The re-rating has already started.

Sources

1. Federal Register, CMMC Program final rule (32 CFR 170), Oct 15, 2024 — federalregister.gov/documents/2024/10/15/2024-22905
2. Venable LLP on the 48 CFR rule effective Nov 10, 2025, Sept 2025 — venable.com/insights/publications/2025/09; Strike Graph, "CMMC Phase 2 deadline November 2026," June 16, 2026 — strikegraph.com/blog/cmmc-phase-2-deadline-november-2026
3. DoD estimate of ~80,000 organizations requiring Level 2; DIB ~221,000 companies — vc3.com/blog/navigating-cmmc-changes-in-2026 (Jan 2026)
4. Cyber AB May 2026 Town Hall: 1,391 final Level 2 certificates — cmmc.com/newsroom/cyber-ab-town-hall-05-2026 (May 27, 2026)
5. C3PAO and assessor counts — tds-is.com marketplace guide (May 13, 2026); intersecinc.com on assessment backlog (early 2026)
6. Backlog projections and remediation timelines — securityboulevard.com, "The November 2026 CMMC deadline" (June 2026); theodosian.com (2026)
7. L3Harris Missile Solutions supplier notice, July 30, 2026 deadline — secureframe.com/hub/cmmc/enforcement-news (2026)
8. Elbit America open letters, Nov 2025–Feb 2026 — elbitamerica.com and secureframe.com/hub/cmmc/enforcement-news
9. Redspin second annual DIB readiness report: 47% received flow-downs — redspin.com (Nov 2025)
10. PwC US Deals 2026 midyear outlook: A&D deal values, PE roll-up thesis, $1.36T prime backlog — pwc.com (June 17, 2026)
11. CRS R48860: FY2026 defense appropriations plus reconciliation — congress.gov/crs-product/R48860 (2026)
12. FY2026 $13.4B AI/autonomy budget line — cdomagazine.tech; meritalk.com (June 2025)
13. CDAO frontier AI awards up to $200M each: OpenAI, Anthropic, Google, xAI — defensescoop.com (July 14, 2025)
14. GenAI.mil launch and ~1.5M users — war.gov (Dec 2025); defensescoop.com (June 12, 2026)
15. ChatGPT at IL5 for 3M+ personnel, early July 2026 — nextgov.com (June 2026)
16. Department AI-first strategy, 30-day model deployment mandate — media.defense.gov AI strategy (Jan 2026); hklaw.com analysis (Feb 2026)

17. FY26 NDAA AI model assessment requirements — wilmerhale.com (Dec 19, 2025)
18. "Slouching toward vendor lock" — federalnewsnetwork.com commentary (June 2026)
19. Defense-tech VC $14.6B in five months — news.crunchbase.com (June 2026)
20. Certification premium of 1.5–2.5x EBITDA turns (directional; single advisory source) — ctacquisitions.com metal fabrication M&A multiples (2026)
21. Defense electronics ~18.7x EV/EBITDA — carlsquare.com; datasite.com (2025–2026)
22. Projected 33,000–44,000 supplier exits (forecast, not observed) — strikegraph.com predictions (Dec 17, 2025)
23. Compliance cost ranges $98K–$305K first year — cispoint.com (Jan 26, 2026); cmmc.com cost guide
24. Elbit: fewer than 1% of 1,000+ suppliers walking away — secureframe.com/hub/cmmc/enforcement-news (2026)
25. CMMC delay history and waiver posture — secureframe.com timeline; DoD May 2025 implementation memo via cmmc.com
26. Gartner 2025 Hype Cycle (GenAI in trough); Deloitte 2026 A&D outlook on pilot scaling — deloitte.com (late 2025)
27. MIT "GenAI Divide" report: ~95% of pilots show no measurable return — fortune.com (Aug 18, 2025)