How to Make The CMMC Phase 2 Pause a Business Opportunity

Stuart Itkin
Aethon Security

The Groundwork

CMMC Level 2

Certification is More Than

Compliance

It’s Proof that an

Organization Can Be

Trusted with the Work

Cost, Schedule, Performance are Only Effective in a Secure Environment

AETHON SECURITY

CMMC Phase 2 Suspension

Effective July 13, 2026 · 60-day CIO review underway

What's Changed

- Phase 2 rollout is paused, including the November 2026 transition deadline
- Only CMMC Level 1 (Self) or Level 2 (Self) may appear in new procurement requirements
- Level 2 (C3PAO) and Level 3 (DIBCAC) designations may not be used during the pause
- Existing solicitations and contracts with C3PAO or DIBCAC requirements must be amended to remove them
- No waivers for higher assessment levels will be granted during the review
- A CMMC Reform Task Force is running a 60-day review to redesign the program

What Hasn't Changed

- Baseline compliance with NIST SP 800-171 Rev 2 is still required
- DFARS 252.204-7012 safeguarding and cyber incident reporting stays in effect
- FAR 52.204-21 basic safeguarding for federal contract information still applies at Level 1
- Level 1 (Self) and Level 2 (Self) assessments can still be required in solicitations
- Other contractual cybersecurity clauses remain intact
- No-cost support (DoW Cyber Crime Center, NSA CCC, Project Spectrum) stays available

AETHON SECURITY

The Pause is a Head Start, Not a Holiday

The government may have paused a certification deadline, but it did not pause cybersecurity obligations, prime contractor requirements, or competitive pressure.

- NIST SP 800-171 and DFARS requirements remain in force.
- Primes continue to evaluate supplier cyber maturity.
- Contract opportunities continue to require proof of cybersecurity readiness.
- Organizations that use the pause wisely will emerge ahead of competitors when requirements return.
- Organizations that stop will simply have less time, more risk, and fewer options.

The pause changed the calendar. It did not change the direction of travel

AETHON SECURITY

Not a Compliance Program. A Market Access Strategy.

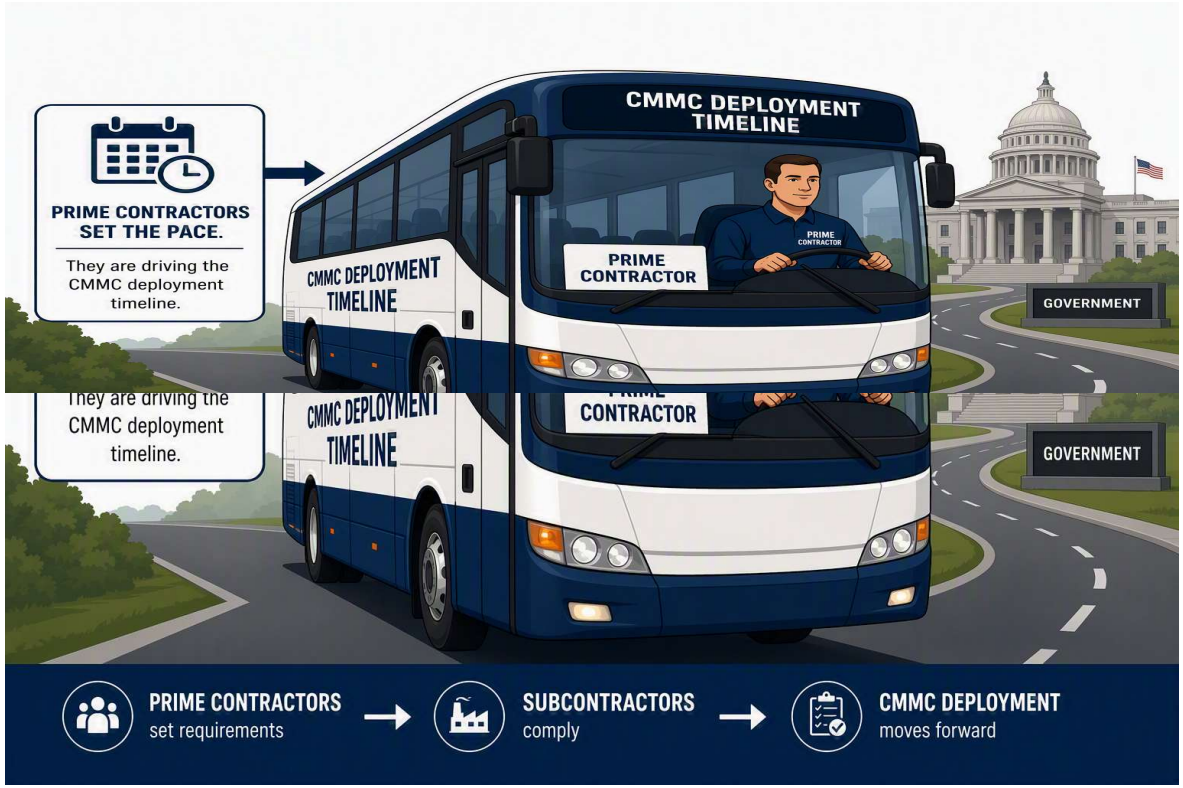
The primary value of CMMC Level 2 is not passing an assessment. The value is remaining eligible for opportunities others cannot pursue.

Benefits

- ✓ Eligibility for CUI-related opportunities
- ✓ Reduced risk of procurement disqualification
- ✓ Improved standing with primes
- ✓ Greater confidence from government buyers
- ✓ Ability to pursue larger and more sensitive contracts

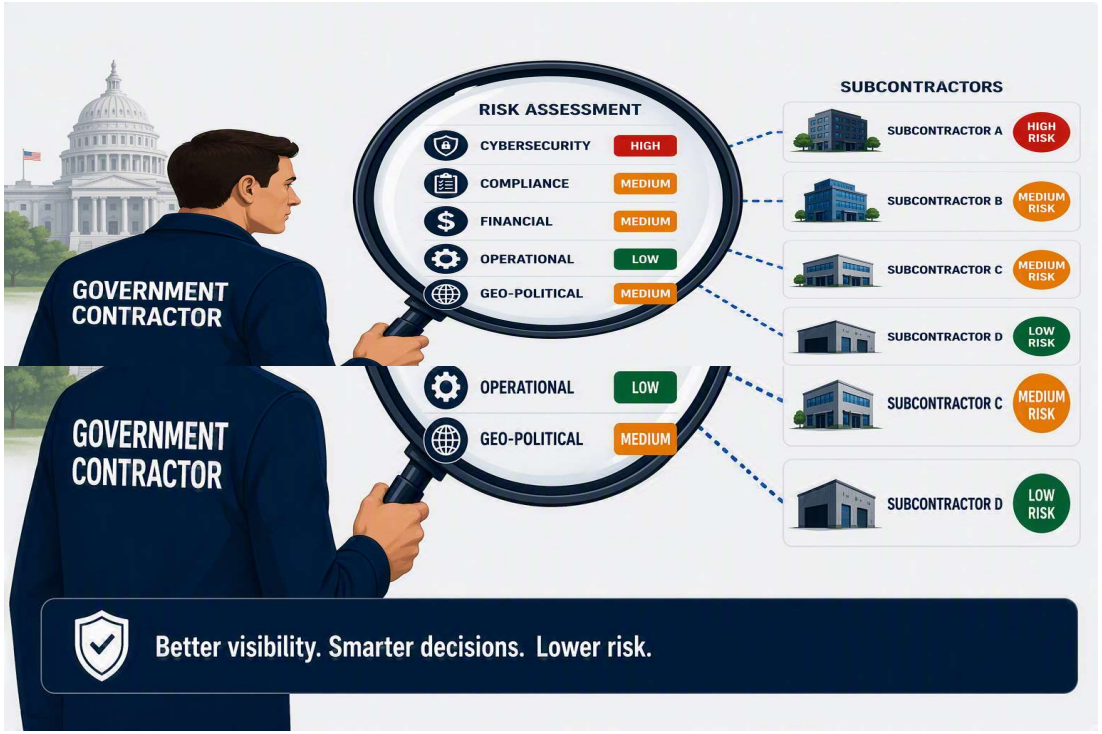
AETHON SECURITY

Who Is Driving The Bus?



AETHON SECURITY

Primes Look at Subs Through a Risk Lens



AETHON SECURITY

What One Prime is Saying

How can getting a level 2 CMMC certification even right now become a competitive advantage for a small business and enable them to win more business either as a sub or a prime?

"So, I know that in my world, when I go and I'm looking for business partners, I ask for it. As the CIO of a publicly traded company, I ask for it.
If you're going to come and do work with me. I am not going to spend my time, my dollars, my small IT budget, going out to make sure you're okay, that's your job.

You need to come to the table ready to play. That's what I would tell everybody . . .IonQ takes it very seriously on my supply chain, that if you're working with me, you better be at level 2."

AETHON SECURITY

Primes Response to CMMC 2.0

- Primes were accelerating CMMC adoption — suppliers were being told to document status, close gaps, and prepare for certification to remain eligible for future work.
- L3Harris: Suppliers handling CUI were expected to **achieve CMMC Level 2 by July 30, 2026**, or risk exclusion from affected programs.
- Elbit: Building network of L2 certified suppliers asked suppliers with SPRS L2 CMMC UID to submit for onboarding onto CMMC-approved supplier list
- Leonardo DRS: Urged suppliers to continue CMMC preparation immediately, emphasizing that cybersecurity readiness would impact future qualification and opportunities.
- Lockheed Martin: Suppliers without demonstrated CMMC maturity face greater risk scrutiny, while Level 2-ready suppliers are better positioned for RFQs, bids, and renewals.

AETHON SECURITY

Primes are Continuing to Drive the Bus

Major primes continue to maintain supplier requirements tied to C3PAO-assessed CMMC Level 2 certification.

- Elbit (7/16/26): Suppliers told not to delay compliance; CUI suppliers should obtain L2 certification as soon as possible.
- L3Harris Missile Solutions: Maintained a 7/30/26 L2 certification deadline; no public rescission identified.
- Leonardo DRS: L2 certification through a C3PAO remains a pre-award requirement for suppliers handling CUI.
- General Dynamics Land Systems: CUI suppliers must achieve CMMC Level 2 and complete audits through accredited third parties.
- BPMI: Evidence of C3PAO L2 certification remains a condition of contract award and supplier eligibility.

BPMI

Elbit Systems

GENERAL DYNAMICS Land Systems

L3HARRIS

LEONARDO DRS

AETHON SECURITY

Why a CMMC L2 C3PAO Certification is an Opportunity

89%	Of DIB experienced business impacts from a cyber incident[1]
1%	Of the DIB is fully prepared for CMMC[1]
47%	Receiving prime contractor flow down requirements[2]
42%	Have submitted an SPRS score[1]
60 of 110	Median SPRS score[1]
17%	Reported a negative SPRS score[1]
25%-40%	Higher win rates for certified contractors[3]
10%-20%	Price Premium[3]
10%-20%	Cyber insurance benefit[4]

[1] CyberSheath State of the DIB Report, 2025
[2] RedSpin CMMC Research Report, 2025
[3] Mytech: IBSSCORP Benchmarking, 2026
[4] Time2Accelerate, The Real Cost of CMMC Compliance, 2025

AETHON SECURITY

DOW is also Looking at Risk: DFARS 252.204-7024

Notice on the Use of the Supplier Performance Risk System.

As prescribed in 204.3 pt ON THE USE OF THE SUPPLIER PERFORMANCE RISK SYSTEM (MAR 2023)

(a) *Definitions.* As used in this provision—

"Item risk" means the probability that a product, based on intended use, will introduce performance risk resulting in safety issues, mission degradation, or monetary loss.

"Price risk" means a measure of whether a proposed price for a product or service is consistent with historical prices paid for that item or service.

"Supplier risk" means the probability that an award may subject the procurement to the risk of unsuccessful performance or to supply chain risk (see Defense Federal Acquisition Regulation Supplement 239.7301).

(b) The Supplier Performance Risk System (SPRS), available at https://piee.eb.mil/, will be used in the evaluation of the Quoter or Offeror's performance. SPRS retrieves item, price, quality, delivery, and contractor information on contracts from Government reporting systems in order to develop risk assessments.

(c) The Contracting Officer will consider SPRS risk assessments during the evaluation of quotations or offers received in response to this solicitation as follows:

(1) Item risk will be considered to determine whether the procurement represents a high performance risk to the Government.

(2) Price risk will be considered in determining if a proposed price is consistent with historical prices paid for a product or a service or otherwise creates a risk to the Government.

(3) Supplier risk, including but not limited to quality and delivery, will be considered to assess the risk of unsuccessful performance and supply chain risk.

(d) SPRS risk assessments are generated daily. Quoters or Offerors are able to access their risk assessments by following the access instructions in the SPRS user's guide available at https://www.sprs.csd.disa.mil/reference.htm. Quoters and Offerors are granted access to SPRS for their own risk assessment classifications only. SPRS reporting procedures and risk assessment methodology are detailed in the SPRS user's guide. The method to challenge a rating generated by SPRS is also provided in the user's guide. SPRS evaluation criteria are available at https://www.sprs.csd.disa.mil/pdf/SPRS_DataEvaluationCriteria.pdf.

(e) The Contracting Officer may consider any other available and relevant information when evaluating a quotation or an offer.

AETHON SECURITY

Don’t Forget the False Claims Act

The suspension of CMMC Phase 2 does not remove your compliance obligations or eliminate legal risk. False certification can lead to severe civil and criminal penalties under the False Claims Act.

Submitting false claims or certification results can result in:

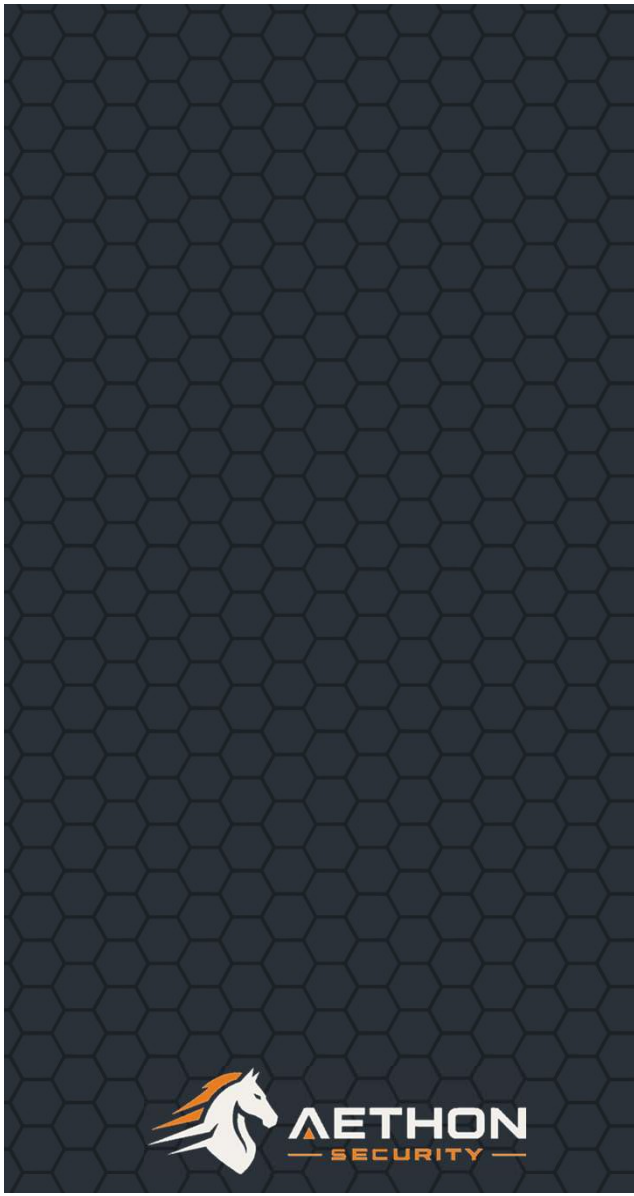
- Civil penalties up to $28,619 per claim
- Treble damages – 3 times the government’s loss
- Criminal penalties – Fines and imprisonment for willful violations

AETHON SECURITY

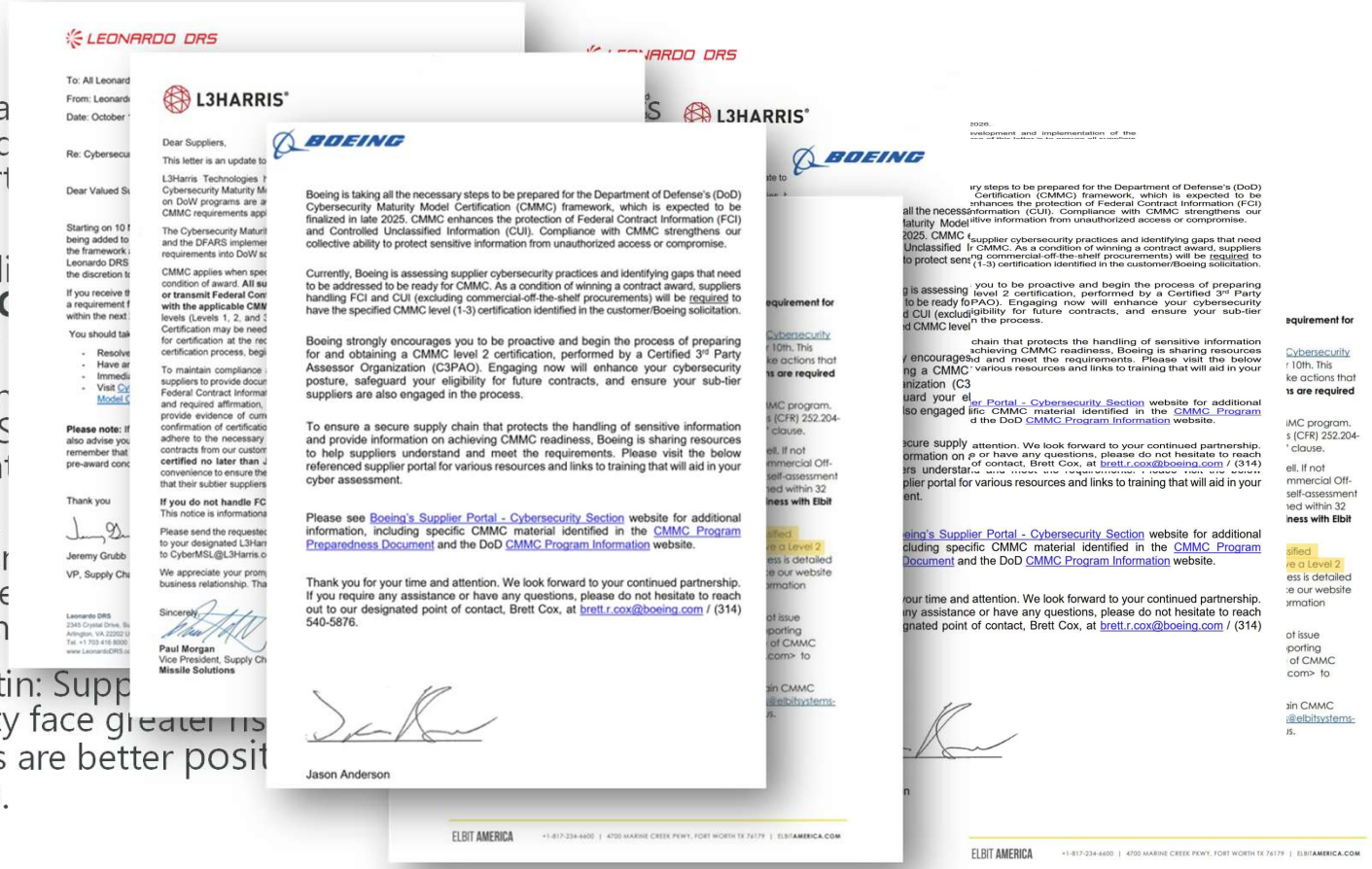
KEY TAKEAWAY

The contractors who treat the pause as a holiday will spend the next phase catching up. The contractors who treat it as a head start will spend the next phase winning business

Primes and the DOW are both considering your cybersecurity posture today when awarding business



Questions?

AETHON SECURITY

- Primes were a
were being tolc
prepare for cert
work.
- L3Harris: Suppli
achieve CMMC
exclusion from
- Elbit: Building r
suppliers with S
onboarding ont
- Leonardo DRS:
preparation imr
cybersecurity re
qualification an
- Lockheed Martin: Supp
CMMC maturity face greater ris
ready suppliers are better posit
and renewals.