ASSESSMENT · SB-2026-01

The Deadline Went Away. The Obligations Did Not.

What the July 2026 CMMC suspension means for a defense contractor.

PUBLISHED 20 JULY 2026 STATUS PUBLISHED REVISED 20 JULY 2026 VERSION 1.3

AUTHOR COLLIN B. GEORGE, CISSP

UNCLASSIFIED // OPEN SOURCE

Analytic record

TYPE	Assessment — a time-bound judgment on a moving regulatory position, superseded when the CMMC Reform Task Force reports.
GOVERNING JUDGMENT	The suspension removed a scheduled verification event. It did not remove any underlying security obligation, the SPRS score requirement, or the annual affirmation.
PROBABILITY	The judgment that no operative legal obligation changed is assessed as almost certain.
ANALYTIC CONFIDENCE	High for the clause analysis, which rests on published regulatory text. Moderate for the enforcement inference, which rests on a settlement record that is small and visible only where the government chose to publicize it. These are separate axes and are not combined.
SUPERSESSION	Reassess on the Task Force report, expected mid-September 2026.
REVISION HISTORY	1.0, 20 July 2026 — first publication. 1.1, 20 July 2026 — added executive summary; recorded that two memoranda issued on 13 July 2026 rather than one; corrected the description of the companion analytic version. 1.2, 20 July 2026 — recorded the Brilliant at the Basics interim guidance campaign and its relationship to the continuing obligations. 1.3, 20 July 2026 — corrected the version stated in the suggested citation; removed an assertion that the companion instrument accompanies this briefing, which it does not; repaired a sentence fragment in the limitations; normalised spelling and date format in prose. No finding changed in any revision.

Executive summary

- The suspension removed a scheduled outside audit. It removed no underlying security obligation.
- Four duties continue unchanged: protect controlled information and report incidents within 72 hours; meet the 110 requirements in NIST SP 800-171 Rev 2; self-score and post that score in SPRS; and sign an annual affirmation, by name, as a senior official.
- A posted score and an affirmation are statements made to the government on a date. They stay on the record and can remain relevant for years under the False Claims Act.
- Whatever the 60-day review decides applies going forward. It does not reach a statement already made.
- A score can be accurate and still indefensible. If you cannot reconstruct how you reached it — which requirements, what evidence, who decided — you cannot show it was reasonable when it was made.

On July 13, 2026, the Department of War suspended the rollout that would have required many defense contractors to pass an outside cybersecurity audit. Contractors subject to these requirements have already been assessing themselves against the government's security standard and posting the resulting score. Third-party certification would have added an outside layer of verification for certain contracts. That requirement — certification under the program known as CMMC — was scheduled to start appearing in contracts on November 10, 2026. It is now on hold while a task force spends sixty days reviewing whether the program should continue

in its present form. The Department stated that the program had created prohibitive compliance costs and bureaucratic burdens, and cited Small Business Administration data indicating that compliance was pushing companies out of the defense industrial base.[1]

What was principally suspended is the scheduled certification layer. The underlying security requirements, self-assessments, and government authority to assess contractors remain. The Department said in the same announcement that the action does not eliminate the requirement for companies to protect federal data.[1] Every underlying security obligation your company carried on July 12 it still carried on July 14. What went away is the scheduled check — the date on the calendar that would have forced you to look closely at your own numbers. The unscheduled one remains. The Department said it will keep enforcing the same standard through company self-assessments and through select government-led assessments, and the government's own assessors kept every bit of the authority they had before.

> **That distinction matters more than anything else in this briefing. Nobody is going to make you look at your own position. The government can still look at it whenever it chooses.**

Four Things You Still Have to Do

Nothing on this list changed on July 13.

1. **Protect controlled information.** You must provide adequate security for the sensitive government information on your systems, and report a cyber incident to the Department within 72 hours of discovering it. The clause is DFARS 252.204-7012.[2]
2. **Meet the technical standard.** Access controls, logging, encryption, multifactor authentication, and the rest — 110 requirements in total. The standard is NIST SP 800-171, Revision 2, which the Department named specifically as what it will enforce during the review.[1]
3. **Score yourself and post the score.** You assess your own implementation of those 110 requirements, and the number goes into the Department's contractor database, the Supplier Performance Risk System. Everyone calls it SPRS.
4. **Sign an annual affirmation.** Once a year, a named senior official affirms that the company continues to meet the requirements associated with its CMMC status. Not the compliance team — a person, by name, with authority to make that statement. The rule is 32 CFR 170.22, and the suspension did not touch it.[3]

The fourth item is the one most often treated as paperwork. It deserves direct executive attention because it attaches a named senior official to the company's continuing representation.

The Department also announced an interim guidance campaign, Brilliant at the Basics, intended to help smaller companies secure their information technology and operational technology. It is guidance, not regulation. It does not replace the 110 requirements, does not change what you have already represented, and following it is not an answer to a representation that was inaccurate when it was made.[10]

Your Contracts Probably Cite Two Different Sets of Clause Numbers

In February 2026, months before the suspension and unrelated to it, the government renumbered the cybersecurity clauses as part of a broader rewrite of federal acquisition regulations. This was done through Class Deviation 2026-O0025, issued by the Defense Acquisition Regulations System, rather than through completed rulemaking.[4] FAR 52.204-21 became FAR 52.240-93. DFARS 252.204-7020 became DFARS 252.240-7997. DFARS 252.204-7019 is no longer prescribed for new solicitations under that deviation, though it remains in the codified regulation. The requirements did not change. Only the numbers did.

A renumbering cannot reach backward and rewrite a contract already signed. So if you hold contracts from before February 1, 2026 and contracts from after, you are operating under two sets of clause numbers at once. Many companies hold both and have not noticed.

A second revision issued on July 16, 2026, and what it changed has not yet been publicly established. So the action item is not to consult a crosswalk. Published crosswalks go stale, and this one may already have. Read the clause list in your own contracts.

You Have Already Made Statements to the Government, and They Are Still on the Record

This is the part of the picture that most coverage of the suspension has left out.

Your posted score is not merely a status indicator. It is a statement submitted to the government on a specific date. An annual affirmation is likewise a statement made by a specific named official. Those statements may eventually expire for award or certification purposes, but they do not disappear. They remain part of the government record and may still matter if the accuracy of an earlier representation is later questioned.

The relevant legal exposure can extend for years. Under the False Claims Act, an action generally must be brought within six years of the violation, or within three years after the responsible government official knew or reasonably should have known the material facts, subject to a ten-year outer limit.[5] That does not mean every score or affirmation creates a separate violation. It means earlier representations may remain relevant long after they are replaced by newer ones.

If your company posted an assessment and later renewed or supplemented its representations, the government may examine each statement against the requirements, evidence, and company knowledge that existed when it was made.

Whatever the Review Decides, It Only Applies Going Forward

The task force reports to the Department's Chief Information Officer around mid-September. It could recommend keeping third-party certification on a later schedule, replacing it with something else, or reducing the number of requirements companies have to meet. The Department's public request for industry input leaves all of those open. That request is a formal Request for Information posted on SAM.gov, and responses close at noon Eastern on August 14, 2026.[6]

None of it reaches backward. If the rules are relaxed in October, that changes what you have to do in November. It does not make a statement you made in 2023 correct. A statement is judged against the requirements that applied when it was made.

This is why the question in front of you does not resolve itself in September. Waiting for the review answers what you will owe next year. It does not touch what you have already said.

A Score Can Be Right and Still Be Indefensible

Consider a company that posted a score of 92. The 92 was accurate. The controls were genuinely in place. Three years later, the person who did the scoring has left, the worksheet was on a laptop that was reimaged, and nobody remaining can say which requirements were counted as met, what evidence supported each one, or who made the call.

That company may be unable to substantiate its score if challenged. Not because the score was wrong, but because it can no longer show that the score was reasonable when it was made. Those are different problems, and only the second one is fixable after the fact.

The same distinction runs through the technical side. Say your company has genuinely enforced multifactor authentication on every remote and privileged login for years. It works, it is real, and everyone uses it. If you cannot produce reliable evidence that it was implemented and operating as claimed, an assessor may be unable to credit the requirement as met. The control exists. The proof does not. To anyone reviewing you, those look identical.

Missing evidence is not the same as a missing control. But in an assessment, it can produce the same result.

What It Has Cost the Companies That Got It Wrong

Five kinds of consequence attach.

You can lose award eligibility. For contracts subject to NIST SP 800-171 assessment requirements, the government verifies that a current score is posted in SPRS before award or option exercise. Where a contract also requires a particular CMMC status, the required status and associated affirmation must remain current. A lapse can cost you a renewal without anyone alleging anything.

You can face contract action — cure notices, withheld payment, termination.

You can face False Claims Act liability. Damages are tripled, plus a penalty per claim submitted. Cases can be brought by the government or by a private whistleblower, who keeps between fifteen and thirty percent of the recovery. In fiscal year 2025 the government recorded 1,297 whistleblower filings, the highest number ever, and DOJ reported recoveries of more than $52 million across nine cybersecurity settlements.[7]

The person who signed can be exposed personally. The statute reaches anyone who knowingly makes a false statement material to a claim for payment, and "knowingly" is defined to include reckless disregard for whether the statement is true. Lying is not required. Signing without a basis can be enough. The rule defines the signer as the person responsible for ensuring compliance, which makes it harder to argue they were only relaying what technical staff told them — though a title alone establishes nothing. The government still has to prove what the person knew or disregarded.[5]

And it can follow the company after you sell it. In a resolution announced May 1, 2025, Raytheon, its parent, and the company that had acquired one of its business lines paid $8.4 million. The alleged conduct ran from 2015 to 2021. The business was sold in March 2024. The settlement named the acquiring company as successor in liability anyway.[8] Restructuring did not separate the buyer from the exposure.

The clearest illustration is the most recent. In June 2026, a Huntsville defense contractor called LOGZONE resolved allegations arising from a self-assessed score of 110 — the maximum possible. A later government assessment, conducted by the Defense Contract Management Agency, scored the same company at negative 170. It paid $507,144. It had received approximately $682,000 on the two Navy contracts at issue.[9]

Two details about that case are worth noting. LOGZONE was not identified through a certification assessment. The publicly available resolution attributes discovery of the deficiencies to a DCMA assessment of the kind that still happens today, unaffected by the suspension. And like most of these matters, it resolved without any admission of wrongdoing — which means the resolution says nothing about whether the company did anything deliberately, and the cost was the same either way.

Most of What Goes Wrong Is an Error, Not a Lie

If you read the section above and recognized something in your own company, the odds are strongly against it being misconduct.

The common failures are ordinary. Scoring the 110 requirements involves judgment calls, and reasonable people applying the same methodology reach different numbers. Controls get implemented properly by competent people who never write down that they did it. The boundary of where sensitive government information actually lives in a company is genuinely difficult to determine, especially in a business where engineering, contracts, and email all touch the same files. And a great many companies reasonably concluded that moving to a government-authorized cloud platform covered their obligations, when in fact

the platform satisfies part of the requirement set and the rest still has to be implemented and documented by the contractor. That last one is a misreading of a genuinely unclear allocation, not a shortcut.

None of these are fraud. All of them produce a gap between what you told the government and what you can currently prove.

The distinction that matters when you go looking is between four situations: the control is in place and documented; the control is in place but undocumented; the control was described differently than it actually works; and the control is not in place. The second you can document going forward yourself; establishing what supported the earlier statement is harder and sometimes cannot be done. The fourth involves the accuracy of something you already submitted, and it is not a technical decision.

Before the Next Affirmation Is Signed

The person signing should be able to state what they relied on. Not in general terms — specifically. What review was performed, when, by whom, what remained open, and why the open items do not defeat the certification they are about to make.

That record needs to exist before the signature, not after someone asks for it. A contemporaneous, documented basis is important evidence against an allegation that the signer acted with reckless disregard. Assembled afterward, it carries considerably less weight.

This is a modest amount of work if the underlying assessment is sound and a revealing amount of work if it is not. Either result is worth having before the signature rather than after.

When to Stop and Call a Lawyer

If you look into this and find that a score or an affirmation already submitted may have been wrong, stop.

At that point the questions are no longer technical. Whether to correct the posted score, in what order, whether to tell anyone, and whether to disclose voluntarily are legal questions with consequences that depend on facts specific to your company. Fixing the underlying control is almost always right. What to do about the statement already on the record is not something to decide internally, and it is not something to decide quickly.

This briefing is not legal advice and is not a substitute for counsel.

Three Checks You Can Do This Week

None of these costs anything. All three can be done with information your company already has.

One. Pull your current SPRS score and its date. Know what number is posted against your company right now and when it went up.

Two. Find out who signed the last affirmation, and ask them what they relied on. If they can describe the review, its date, and the open items, that is a good answer. If the answer is that it came around and they signed it, you have found something worth addressing before the next one.

Three. Determine whether the worksheet behind your posted score still exists. Not the score. The requirement-by-requirement determination that produced it.

If all three come back clean, you have cleared the first representation-defensibility check. That does not establish full technical compliance, but it means the company can identify what it represented, who approved it, and the record supporting the score. That is a real outcome and it is more common than the enforcement record suggests, because settlements are the only cases anyone publishes.

If any one of the three cannot be answered, that is the finding. It does not mean you have a problem. It means you cannot presently tell whether you have one, and that condition is worth resolving deliberately rather than discovering under a demand. A companion instrument, the Representation Defensibility Matrix, works through it in order — statement by statement, from what you said, to what would support it, to what you actually hold. It is available on request.

LIMITATIONS

What this assessment does not establish

This assessment addresses the legal and evidentiary position of contractors under representations already made. It does not assess whether third-party certification improved cybersecurity outcomes across the defense industrial base, whether the suspension will increase or decrease compromise, or what the Department should do. Those are different questions.

The enforcement record it draws on consists of settled and publicly announced matters. Settlements over-represent resolutions the government chose to publicize and under-represent declinations, investigations closed without action, and matters resolved under seal. The visible pattern may describe the announced layer accurately and the decisive layer poorly.

Two facts material to the analysis are unresolved in the public record. The CMMC Reform Task Force has not reported, so what replaces the suspended requirement is unknown. A second revision to the clause renumbering issued on July 16, 2026, and its effect is not yet publicly established. Neither is treated here as settled.

An assessment that cannot state what would change it should not be published. This one would change if the Task Force recommended retaining third-party assessment on a revised schedule, if a Department of Justice action were premised on an affirmation submitted after July 13, 2026, or if the affirmation obligation itself were amended by rulemaking or class deviation.

SOURCES

Primary sources

Every factual assertion traces to a primary regulatory, statutory, or Department of Justice record. Where the public record does not settle a question, the text says so rather than resolving it by inference.

1 Department of War, Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements (13 July 2026). Two memoranda issued: the suspension memorandum signed 10 July 2026 by DoW Chief Information Officer Kirsten A. Davies, and a separate memorandum from the Under Secretary of Defense for Acquisition and Sustainment directing program officers to remove third-party certification requirements from active solicitations.

2 DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

3 32 C.F.R. § 170.22 (affirmation of continuing compliance); 48 C.F.R. § 204.7501 (currency of CMMC status). The 32 C.F.R. Program rule took effect 16 December 2024; the 48 C.F.R. acquisition rule took effect 10 November 2025.

4 Class Deviation 2026-O0025, Revolutionary FAR Overhaul — FAR Part 40, DFARS Part 240, Defense Acquisition Regulations System, effective 1 February 2026; Revision 2 issued 16 July 2026.

5 31 U.S.C. §§ 3729–3733. Scienter defined at § 3729(b)(1) to include reckless disregard; limitations at § 3731(b).

6 Department of War, Request for Information on CMMC reform, posted to SAM.gov 13 July 2026. Responses due 12:00 p.m. ET, 14 August 2026.

7 U.S. Department of Justice, Fact Sheet: False Claims Act Settlements and Judgments, Fiscal Year 2025 (16 January 2026). The 1,297 qui tam figure and the 15–30 percent relator share appear in the accompanying press release. https://www.justice.gov/opa/media/1424126/dl

8 U.S. Department of Justice, Raytheon Companies and Nightwing Group to Pay $8.4 Million to Resolve False Claims Act Allegations Relating to Non-Compliance with Cybersecurity Requirements in Federal Contracts (1 May 2025). Alleged conduct 2015–2021; the business was sold in March 2024. https://www.justice.gov/usao-dc/pr/raytheon-companies-and-nightwing-group-pay-84-million-resolve-false-claims-act

9 Settlement agreement, United States v. LOGZONE, Inc. (June 2026), recording the October 2021 self-assessed score of 110 and payment of $682,193.37 under the NAVOCEANO contracts; U.S. Department of Justice release of 18 June 2026. https://www.justice.gov/opa/media/1446716/dl

10 Department of War announcement of 13 July 2026 establishing the Brilliant at the Basics campaign. Chief Information Officer Kirsten Davies described it as guidance for securing information technology and operational technology environments, with the stated aim of enabling small businesses to protect their operations without a large compliance overhead. The content of the associated IT and OT lists was not established in the public record at the time of writing.

SUGGESTED CITATION

George, Collin B. The Deadline Went Away. The Obligations Did Not. Assessment SB-2026-01, version 1.3. Sanctir LLC, 20 July 2026.

METHOD

Method note

This briefing is independent open-source analysis. Its findings trace to primary sources: the Department of War announcement of July 13, 2026; the CMMC Program rule at 32 CFR part 170; the DFARS clauses cited; the False Claims Act at 31 U.S.C. 3729–3733; and Department of Justice settlement announcements. Where the public record does not settle a question — including the effect of the July 16, 2026 clause revision and the outcome of the sixty-day review — that is stated rather than resolved by inference.

A longer analytic version underlies this briefing, evaluating competing explanations of the suspension's effect across four contractor populations with full citations. It is available on request. Sanctir is a solo practice; this work was subjected to adversarial self-review, not external peer review.

AUTHOR

About the author

Collin B. George, CISSP, is the principal of Sanctir LLC, an independent research and advisory practice working on CMMC and NIST SP 800-171, export controls, sanctions, and defense industrial base risk.

Sanctir is a solo practice. This assessment was subjected to adversarial self-review rather than external peer review, and is not affiliated with any government agency, academic institution, or defense contractor.

ORCID 0009-0007-8162-6839 · FULL BACKGROUND · CONTACT