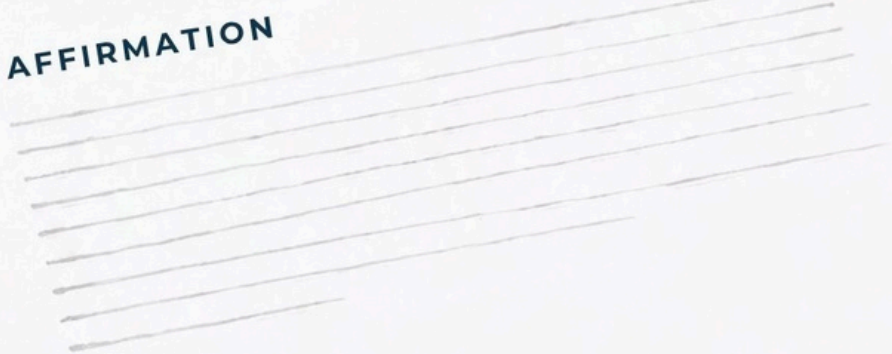
DivIHN
IN SERVICE, WITH EXCELLENCE AND GRACE

Signing the Affirmation

What DoD Contractors Attest To, and Who Answers for It

Practical guidance from CMMC compliance practitioners.
Not legal advice.



2026 CMMC COMPLIANCE GUIDE

Table of Contents

Practicalguidancefor theexecutive whosigns the affirmation — what it asserts, what protects it, and what changed when third-party review came off the table. **Not legal advice.**

4	8	1	Diligence before you sign by name
Parts	Chapters	Signature	

One decision, held by a named person — understand it, build the diligence behind it, and keep it honest.

EXECUTIVE PERSPECTIVE

The Signature Is Personal

Theaffirmation is a short,formal statement to thegovernment that your company meets the cybersecurity requirements of its contracts. It is signed by a named person — the affirming official — and once it is submitted, it represents the company as fact. It is not a checkbox. It is a representation the government can act on, and, if it turns out to be wrong, pursue.

What changed in July 2026 is easy to miss and important to understand. The Department paused the third-party assessment step of CMMC. Much of the market read that as relief — one fewer audit, one lower bill. But for the person who signs, the effect ran the other way: the independent reviewer who used to check the work before it reached the government is, for new work, no longer in the middle. The signature now stands closer to the consequence.

> **The market read the Phase 2 pause as relief. For the person whose name is on the affirmation, it is the opposite — the last check between the company's claim and the government's record has been removed.**

$507,144

LOGZONE, June 2026 —aself-reported perfect SPRS score against a later assessed score of −170.

$8.4M

Raytheon / Nightwing—a settlement citing DFARS 252.204-7012 and FAR 52.204-21, the basis for Level 1.

July 2026

Phase 2paused — third-party review removed for new solicitations; self-assessment remains.

WHO THIS IS FOR

The owner, president or senior official who will sign the affirmation — written to be read without a technical background, because the signature is a governance act before it is a technical one.

WHAT IT DOES

It stays in the lane of what to do: understand the signature, build the diligence to stand behind it, and keep it honest as the business changes. It does not interpret the law.

Not legal advice. This guide is practical guidance from CMMC compliance practitioners on what to do before signing an affirmation. It is not legal advice and does not interpret the law. Enforcement figures are drawn from public government and legal-industry reporting current to mid-2026; confirm them, and your own obligations, with qualified counsel before you rely on them.

PART ONE · THE SIGNATURE

What You Are Actually Attesting To

Strip away theacronymsandtheaffirmationsays somethingsimple and absolute: the required controls are in place **now**. Not planned. Not funded. Not mostly done. The document does not describe a journey or an intention — it describes a present state, on behalf of the whole company, at the moment you sign. Understanding that plainly is the first act of diligence, because everything else in this guide follows from it.

FIGURE 1 · WHAT THE AFFIRMATION ASSERTS

THE AFFIRMATION ASSERTS —

- **Current implementation**
  every required control is in place now, not planned or in progress
- **On the company's behalf**
  the statement binds the organisation, not just the signer
- **For a defined period**
  it speaks to the state of the environment at the time of signing
- **With no POA&Ms at Level 1**
  "partially done" is not an option — it is done, or it is not affirmed

Affirming Official — signature & date

ON WHOSE BEHALF

The affirmation binds the organisation, not just the individual. The signer speaks for the company — which is why the company's leadership, not only its IT function, has a stake in it.

FOR WHAT PERIOD

It states the position at the time of signing. The environment will change; the affirmation does not update itself. That gap is the subject of Part Four.

The word doing the most work is "is". The affirmation is written in the present tense on purpose. Reading it as "we intend to" or "we are working toward" is the single most common misunderstanding — and the one that turns an ordinary signature into an exposed one.

PART ONE · THE SIGNATURE

Current Implementation, Not Intent

AtLevel1thereisno partial credit.Higherlevelsallow a Planof Action andMilestones — a documented way to affirm “implemented, except for these items, which we will finish by this date.” Level 1 does not. The basic safeguarding requirements of FAR 52.204-21 are either implemented or they are not, and the affirmation asserts that they are. A single unmet requirement means the affirmation cannot be made truthfully, whatever the state of the project plan.

THE BASIC SAFEGUARDING REQUIREMENTS, IN PLAIN TERMS

Limit access

Only authorised people, devices and processes reach your systems and the information on them.

Authenticate

Identify and verify users before granting access; control who can do what.

Protect the boundary

Monitor and control what crosses the edge of your network.

Guard the media & physical

Sanitise or destroy media; limit physical access to systems.

Maintain & update

Keep systems patched and protected against malicious code.

Verify it works

Confirm the controls actually operate — not just that they exist on paper.

LEVEL 1 — NO PARTIAL CREDIT

Every basic safeguarding requirement must be implemented before you affirm. There is no mechanism to say “done except for these.” The line is binary, and the signature sits on the “done” side of it.

HIGHER LEVELS — A PLAN IS ALLOWED

Higher tiers permit a Plan of Action & Milestones for a limited set of items. That flexibility does not reach Level 1 — a common and costly assumption.

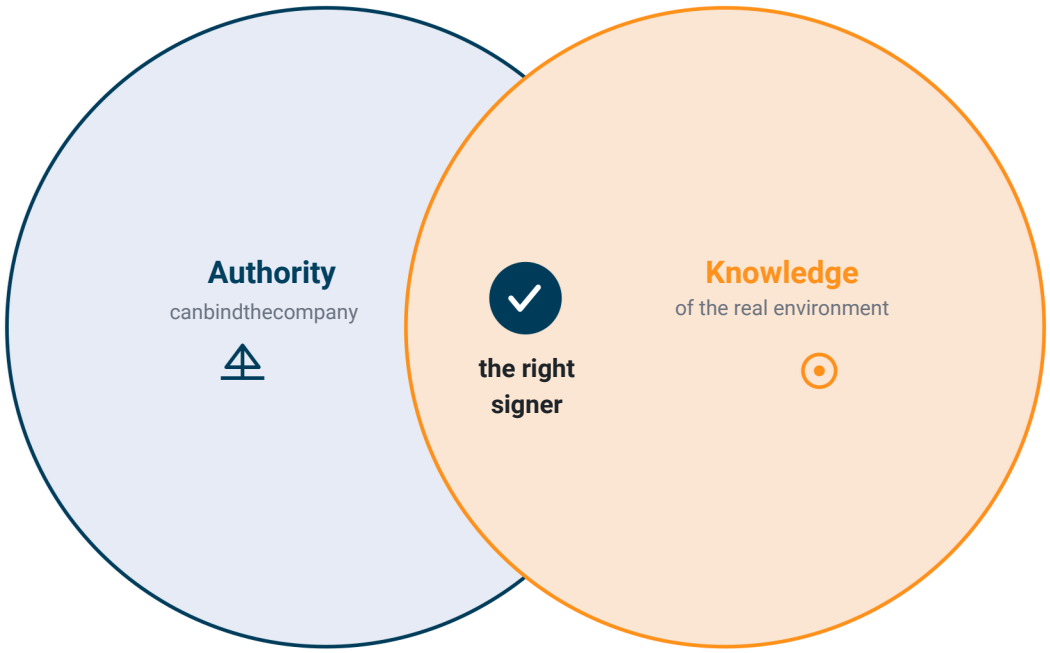
“We are 90% there” is a project status, not an affirmation. At Level 1 the honest options are two: it is done and you can affirm, or it is not and you cannot. Treating that line as firm before you sign is far cheaper than defending a crossed one afterward.

PART ONE · THE SIGNATURE

Who Should Be the Affirming Official

Choosing theaffirming official is agovernancedecisiondressedupasanadministrative one. The signature carries personal weight, so the choice is not simply “whoever has signing authority” or “whoever runs IT.” The right person needs two things at once: the **authority** to bind the company, and enough **knowledge** of the real environment to stand behind what they are asserting.

FIGURE 2 · THE RIGHT SIGNER SITS IN THE OVERLAP



When one person does not hold both, the organisation has to close the gap on purpose — usually by giving the authorised signer verified answers they can trust.

SHOULD NOT SIGN ON AUTONOMY

- Someone with authority but no visibility into the systems
- Someone with knowledge but no standing to bind the company
- Anyone signing on trust alone, without seeing evidence

HOW TO CLOSE THE GAP

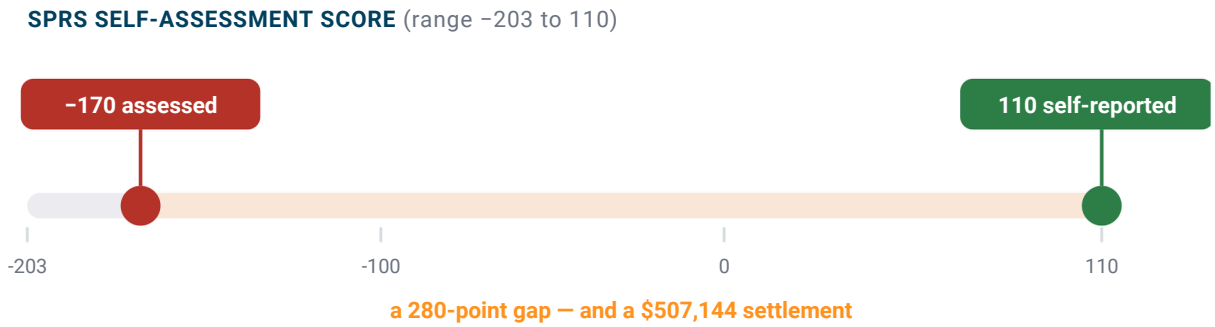
- Pair the signer with the person who did the assessment
- Require the evidence file in front of them before signing
- Record who verified each area, and when

PART TWO · THE RECORD

Enforcement Is Not Theoretical

The clearest evidence thataself-reportedscoreis treated asarealrepresentation is a case that turned on nothing else. In June 2026, an Alabama defense contractor settled False Claims Act allegations for **$507,144**. The government's case rested on the distance between what the company had reported about itself and what a later assessment found — and, notably, there was no whistleblower. The matter surfaced through a government-led review.

FIGURE 3 · A SELF-REPORTED SCORE AGAINST AN ASSESSED ONE



Reported: a perfect 110. Assessed: −170, near the bottom of the −203-to-110 range. The gap between the two is what the government pursued.

WHAT MADE IT ACTIONABLE

A SPRS score is a representation to the government. When the reported figure and the assessed figure diverge that far, the score itself becomes the evidence — no breach or leak required.

WHERE IT CAME FROM

Not a disgruntled employee, but a government audit. That is the detail worth sitting with: you do not need an accuser for a self-report to be tested.

WHAT A SPRS SCORE ACTUALLY IS — AND WHY THIS CASE MATTERS

- A number your company reports about its own security posture
- Submitted to a government system as a formal representation
- Relied on by the government when awarding and paying on contracts
- The **score itself** was the evidence — no breach required
- The gap between reported and assessed drove the case
- The affirming official's job is to make sure that gap does not exist

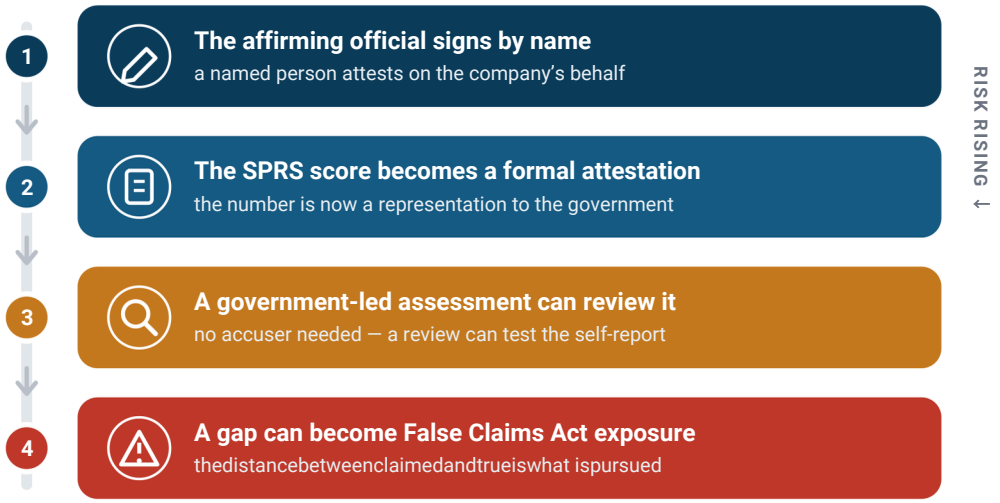
PART TWO · THE RECORD

What the Settlements Signal

Onecaseis ananecdote;a pattern is aposture. Alongside theSPRS matter sits a larger settlement — **$8.4 million** — resolving allegations that a major contractor and its unit failed to meet cybersecurity requirements on a development system. What makes it relevant here is the pairing it cites: both DFARS 252.204-7012 and FAR 52.204-21. The second of those is the basic safeguarding rule that underpins Level 1.

Read carefully, and without overclaiming: most cyber False Claims Act cases involve higher-level requirements and controlled information. Cite them as evidence of the government's posture toward false cyber representations generally — and let the FAR 52.204-21 matter carry the point that even the foundational requirements are within reach of enforcement.

FIGURE 4 · HOW A SIGNATURE BECOMES EXPOSURE



Each step is ordinary on its own. Together they are the path a self-report can travel from a signature to a settlement.

WHAT THE CASES SHARE

- A representation about cybersecurity the government relied on
- A gap between what was claimed and what was true
- Enforcement under the False Claims Act, not a technical penalty

HOW TO READ THEM — CAREFULLY

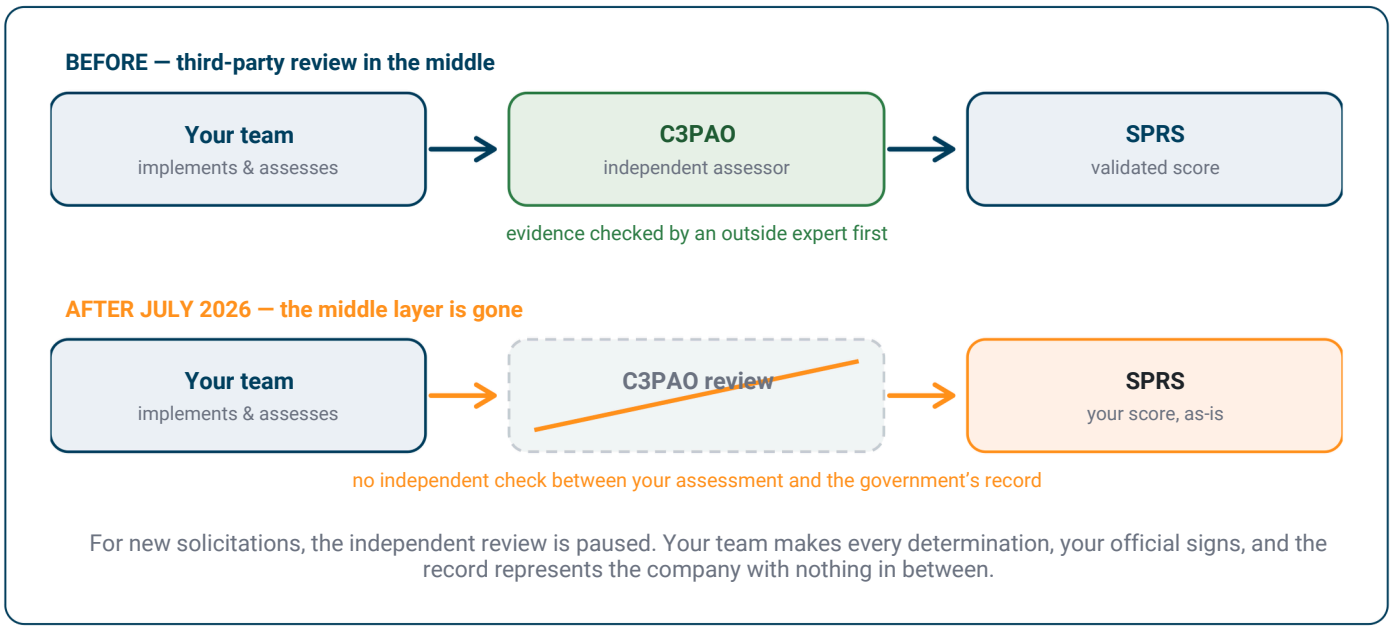
These are not Level 1 rulings, and this guide does not claim they are. They show the direction of enforcement toward false cyber representations — and, through FAR 52.204-21, that the foundational requirements are within its reach.

PART TWO · THE RECORD

Why the Phase 2 Pause Raised Your Exposure

Thisisthereframe that mattersmost,becausealmost nooneissaying itout loud.BeforeJuly2026, a new contractor's path to a compliance record ran through an independent expert. A Certified Third-Party Assessment Organization reviewed the implementation, checked the evidence, and validated the result before it reached the government's system. That layer did two things at once: it caught mistakes, and it stood between your team's judgement and the official record.

FIGURE 5 · THE LAYER THAT USED TO SIT IN THE MIDDLE



WHAT THE ASSESSOR USED TO ABSORB

An independent expert who reviewed the evidence caught honest mistakes before they became official — a buffer that protected the signer as much as the government.

WHY "RELIEF" IS THE WRONG WORD

Removing a cost also removed a safeguard. For the person signing, fewer eyes on the work before it counts is not relief — it is more responsibility, held alone.

Read the pause precisely. **The suspension applies to new Department solicitations; existing contract requirements remain binding until formally modified, and a subcontract that requires a Level 2 third-party assessment still requires it. The self-assessment obligation itself did not go away — only the independent check on it.**

PART TWO · THE RECORD

The Signer Now Stands Alone

Itis tempting to read “paused”as“pausedfor me.”Itis not.The obligations that make the affirmation consequential are still fully in force — what changed is only the friendly expert who used to review your work first. Almost everything that creates exposure stayed the same — and the one thing that moved, moved toward you.

WHAT STILL APPLIES

- Safeguarding covered information under DFARS 252.204-7012
- Submitting self-assessment scores to SPRS
- Reporting cyber incidents within 72 hours via DIBNet
- Existing contract terms, until formally modified
- Subcontract flow-downs that require an assessment

WHAT CHANGED

- No third-party review before your score reaches SPRS, for new solicitations
- Verification shifts toward government-led assessments
- Your self-reported score becomes the primary compliance signal
- The accuracy of that score is now the signer’s to own

The independent assessor was, quietly, a favour to the signer: a second set of expert eyes before anything became official. With it paused, the diligence that assessor used to perform does not disappear — it moves onto your side of the line, to be done and documented before you sign.

WHAT TO DO ABOUT IT — IN PRACTICE

Do the assessor’s job

Assess and verify as rigorously as an outside reviewer would have — because no one else now will.

Document as if reviewed

Build a record that would satisfy an independent expert; assume it may be read by one later.

Treat the score as legal

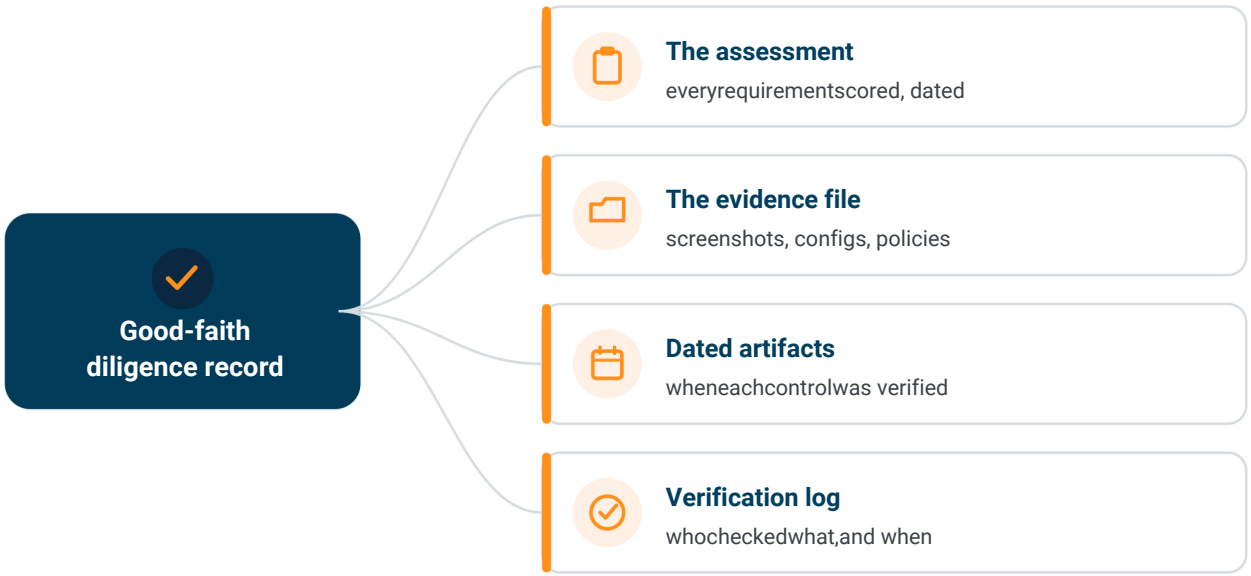
A SPRS entry is a representation to the government. Give it the seriousness that implies, and involve counsel.

PART THREE · BEFORE YOU SIGN

The Diligence Record

Goodfaith isnota feeling; it isafile.If theaccuracyof the affirmation is ever questioned, the difference between a defensible position and an indefensible one is whether you can show the work: what was assessed, what evidence supported each conclusion, and who verified it and when. The point is not to prove perfection — it is to demonstrate that a reasonable, documented process stood behind the signature.

FIGURE 6 · WHAT A GOOD-FAITH DILIGENCE RECORD CONTAINS



Keep it dated and specific. 'We reviewed it' is a memory; a dated artifact with a name against it is a record.

RETAIN, DATED AND SPECIFIC

- The assessment, with every requirement scored
- The evidence behind each "implemented"
- Dates showing when each control was verified
- Names showing who verified what

WHY IT PROTECTS YOU

A contemporaneous, dated record is the practical expression of good faith. It shows the affirmation rested on verification, not assumption — and it is far easier to assemble the week you sign than to reconstruct a year later.

PART THREE · BEFORE YOU SIGN

“IT Handles It” Is Not a Defence

Themostcommonway anexecutiveends up exposedis the mostreasonable-sounding: they trusted that IT, or an outside provider, had it covered. Delegation is fine — but the signature is not delegable, and “I was told it was fine” is a weak place to stand. You do not need to become technical. You do need to ask a few plain questions and recognise an answer that should stop you signing.

QUESTIONS TO PUT TO IT OR YOUR MSP — AND WHAT YOU WANT TO HEAR

Ask	A good answer	A red-flag answer
“Are all the required controls implemented today?”	“Yes — here is the list, each one confirmed.”	“Basically” · “we’re close”
“Can you show me the evidence?”	A dated evidence file, artifact by artifact	“Trust me” · “it’s all in my head”
“Who verified this, and when?”	A name and a recent date per area	“It’s always been fine”
“What are we not doing that we should be?”	A short, honest list — or a clear “nothing”	Silence, or “nothing, don’t worry”

WHAT YOU DELEGATE

- Doing the technical work
- Running the assessment
- Assembling the evidence

WHAT YOU CANNOT DELEGATE

- The signature itself
- Confirming you saw the evidence
- The decision to sign — or to pause

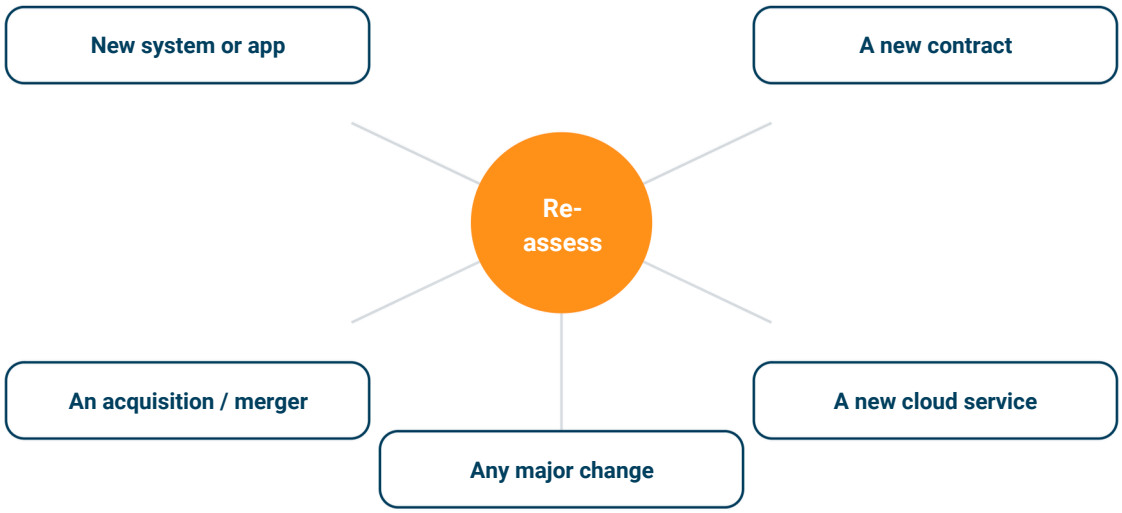
A confident “basically” is the answer to fear most. At Level 1 there is no “basically” — and if the person closest to the systems cannot say “yes, and here is the proof,” the honest move is to pause, not to sign.

PART FOUR · AFTER YOU SIGN

When the Environment Changes

Theaffirmation describesasingle moment.The business doesnotstandstill. A new application goes live, a new contract brings new obligations, an acquisition folds in an unfamiliar environment, a team adopts a cloud service without telling anyone. Each of these can quietly move the company away from the state the affirmation described — and the affirmation does not update itself to keep pace.

FIGURE 7 · WHAT SHOULD TRIGGER A FRESH LOOK



None of these is exotic. Each is a normal event that can change what is true about your environment — and therefore what your affirmation still stands behind.

THE SIGNER'S POSITION IN THE INTERIM

Your affirmation spoke to a point in time. After a material change, the honest position is: the record no longer fully matches the environment — so re-assess the affected area and re-document before relying on the old signature.

MAKE IT SOMEONE'S JOB

Changes slip through because no one owns the question. Name a person who is told when systems, contracts or vendors change — and who decides whether it touches the affirmation.

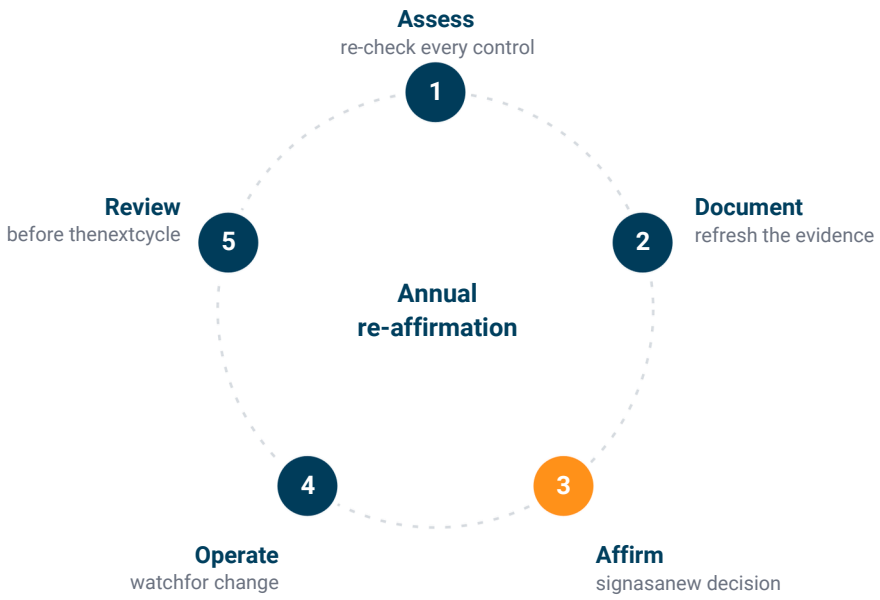
A useful habit: add one line to your change process — "does this affect our affirmation?" Most of the time the answer is no, and it costs a moment. The one time it is yes, that moment is what keeps your signed record and your live environment from drifting apart unnoticed.

PART FOUR · AFTER YOU SIGN

Re-Affirmation as a Decision, Not a Formality

Theaffirmationisrenewedon acycle,and the danger of any cycle is that it becomesahabit. Signingagain "because we signed last year" reproduces last year's risk with none of last year's scrutiny. The healthier frame is to treat each re-affirmation as a fresh determination: a new decision, made against new evidence, about the environment as it stands today.

FIGURE 8 · EACH YEAR IS A NEW DECISION



Assess, document, affirm, operate, review — then begin again. The signature at step three should mean as much the fifth time as the first.

TREAT IT AS NEW

- Re-run the assessment against today's environment
- Refresh the evidence file — new dates, new names
- Account for every change since the last signature
- Decide again, on the merits, whether you can affirm

THE HABIT TO AVOID

A renewal signed on autopilot carries forward every gap that opened during the year — and does so with a fresh date on it, which is the opposite of what you want if the record is ever examined.

APPENDIX

The Pre-Signature Checklist

Onepage to work throughbefore you openSPRS. It doesnotreplace an assessment or legal review — it is the executive's final walk-through, in plain language, to confirm that a signature is warranted and defensible. Governance and scope first; evidence and sign-off overleaf.

GOVERNANCE

- The right person is signing — authority and knowledge
- That person has personally reviewed the position
- Leadership understands the signature binds the company
- Someone owns the affirmation after today
- A named person is told when the environment changes
- Legal review has been obtained where appropriate
- No one is signing on trust alone

SCOPE

- The correct level for each contract is confirmed
- Every in-scope system is accounted for
- Cloud services and vendors in scope are included
- Recent changes since the last review are captured
- Federal contract information locations are known
- Flow-down obligations to subcontractors are reviewed
- Nothing in scope is "assumed" rather than checked

Work top to bottom, and be honest with each line. A box you cannot tick is not a failure of the checklist — it is the checklist doing its job, showing you exactly what to resolve before a signature is warranted.

Reminder. This checklist is a practical aid, not legal advice, and not a substitute for a proper assessment. Confirm your specific obligations with qualified counsel.

Evidence and sign-off continue overleaf →

APPENDIX

Checklist: Evidence & Sign-Off

The secondhalf is wherediligence becomesarecord.Work through it with the evidence file open in front of you — if any line cannot be answered with a dated, specific artifact, that is the line to resolve before the signature, not after.

EVIDENCE

- Every requirement is scored, not assumed
- Each “implemented” has evidence behind it
- Artifacts are dated and specific
- Who verified each area is recorded
- IT / the MSP answered without a “basically”
- No Level 1 requirement rests on a POA&M

SIGN-OFF

- The self-reported score matches the assessment
- The diligence record is retained and findable
- A re-assessment trigger list exists and is owned
- The next re-affirmation is calendared as a decision
- This checklist is completed, dated, and kept
- You can say “yes, and here is the proof” — without a caveat

ONE TEST FOR THE WHOLE PAGE

If the honest answer to any line is “basically”, you are not ready to sign — you are ready to fix.

KEEP THE PAGE

A dated, worked-through checklist is itself part of the diligence record it asks you to build.

THE ONE QUESTION THIS WHOLE GUIDE COMES DOWN TO

“Can I say yes — and show the proof — without a caveat?”

If yes, sign with confidence. If not, you have found your next task, not your signature.

REFERENCE

CMMC Glossary

Plain-languagedefinitionsforthetermsanon-technical signer meets in the affirmation process. For orientation only — not legal definitions.

CMMC
Cybersecurity Maturity Model Certification — the DoD programme that verifies contractor cybersecurity.

Affirming Official
The named person who signs the affirmation on the company's behalf.

Affirmation
A formal statement to the government that required controls are implemented.

Level 1
The foundational tier — basic safeguarding of Federal Contract Information.

Level 2
The tier for Controlled Unclassified Information, based on NIST SP 800-171.

FAR52.204-21
The federal clause requiring basic safeguarding — the basis for Level 1.

DFARS252.204-7012
Requires safeguarding covered defense information and 72-hour incident reporting.

DFARS7019 / 7020
Require submitting and maintaining a self-assessment score in SPRS.

NIST SP 800-171
The control set behind Level 2 and DFARS 7012.

SPRS
Supplier Performance Risk System — where self-assessment scores are recorded.

C3PAO
Certified Third-Party Assessment Organization — the independent assessor now paused.

Phase 2
The third-party assessment phase of CMMC, paused in July 2026.

POA&M
Plan of Action and Milestones — a plan to close gaps; not allowed at Level 1.

FCI
Federal Contract Information — the information Level 1 protects.

CUI
Controlled Unclassified Information — protected at Level 2.

FCA
False Claims Act — the law under which false representations can be pursued.

DIBCAC
The government body that conducts assessments of contractor cybersecurity.

DIBNet
The portal for reporting cyber incidents to the Department.

Government-led assessment
A review conducted by the government rather than a private assessor.

Basic safeguarding
The foundational protections required by FAR 52.204-21.

Covered defense information
Sensitive information DFARS 252.204-7012 requires you to protect.

Self-assessment
Your own evaluation of your posture against the required controls.

Flow-down
A requirement passed from a prime contractor to its subcontractors.

Attestation
A formal statement asserting something is true, relied on by another party.

Diligence record
The dated evidence showing a reasonable process stood behind a signature.

MSP
Managed Service Provider — an outside firm that may run your IT or security.

REFERENCE

About DivIHN

DivIHN helpsdefensecontractors meet their cybersecurity obligations with the documentation to stand behind them. Our CMMC practice works alongside your team and your counsel — assessing the environment, building the evidence record, and preparing the affirming official to sign with confidence rather than hope.

HOW WE HELP

Assessment & evidence

Scoring every requirement and building the dated diligence record.

Affirmation readiness

Preparing the signer with verified answers, not assurances.

Annual renewal support

Re-assessment and affirmation reminders, treated as fresh decisions.

A WORD ON SCOPE

We are cybersecurity compliance practitioners, not attorneys. We help you do the work and document it well; we work with your legal counsel, not in place of them. For any question about legal exposure, that is a conversation for your lawyer — and one this guide is meant to help you have well-prepared.

Signing an affirmation soon?

Talkto DivIHNaboutbuildingthe diligencerecordthatletsyour affirming official sign with evidence behind them.

- divihn.com/cmmc
- CMMC Practice