Managing CMMC With Your Subcontractors

Why Notices to Suppliers Are Not Enough, and What Prime Contractors Should Build Instead

David W. Koran
CyberAB Registered Practitioner Advanced
June 2026

Across the Defense Industrial Base, prime contractors have begun to act on the Cybersecurity Maturity Model Certification. The action visible on the supplier side is almost always the same. A notice arrives. It tells the supplier that CMMC requirements now apply, that the supplier must meet a stated level, and that continued business depends on meeting that level. Some primes attach a questionnaire or a registration form and ask the supplier to attest to its progress. The notice is filed, the form is returned, and the prime records that flowdown has occurred.

A notice is not a solution. It transfers a requirement to the supplier but does nothing to confirm that the supplier can meet it, is meeting it, or will continue to meet it. It moves paper. The controlled drawing still travels to the same small finishing shop it always did, and the question of whether that shop actually protects the information remains unanswered. The prime has shifted the burden downward while keeping the consequence for itself.

This paper makes a single argument. Managing CMMC across a subcontractor base is not a matter of sending notices. It is a continuing management responsibility that requires two things to work together: strategic monitoring of compliance status across every tier that handles controlled information, and active assistance to suppliers that cannot reach or maintain that status on their own. Both belong inside a defined function, with clear ownership, a repeatable process, and verification renewed over the life of the work. The smallest specialty processors, the platers, the anodizers, the heat treat shops, and the testing labs, receive controlled information as a routine part of building a part. They sit at the bottom of the chain, and that is exactly where a notice does the least and where the prime can see the least.

The Regulation Reaches Every Tier

The legal foundation for whole-chain responsibility rests on a two-part CMMC rulemaking that is now fully in effect. The program rule at 32 CFR Part 170 established the CMMC framework, defined the assessment levels, and set the flowdown requirements. It took effect on December 16, 2024. The contract clause that implements the program, DFARS 252.204-7021, took effect on November 10, 2025, and makes a current CMMC status a condition of contract award and of continued performance.

The flowdown provision is 32 CFR 170.23. Its scope statement is direct. CMMC requirements apply to prime contractors and subcontractors throughout the supply chain at all tiers that will process, store, or transmit any FCI or CUI on contractor information systems in the performance of the contract or subcontract. The operative obligation that follows is equally direct. A prime contractor shall comply, and shall require its subcontractors to comply with and to flow down CMMC requirements, such that compliance is required throughout the supply chain at all tiers.

Two features of that language deserve attention.

The obligation cascades. The prime flows the requirement to its subcontractor. That subcontractor, as a condition of its own subcontract, must flow the requirement to the next tier, and onward, for as long as controlled information continues to move down the chain. There is no tier at which the obligation stops on its own. It stops only when the information stops, which for a machined and finished part can be four or five tiers deep.

The required level follows the data, not the position in the chain. Section 170.23 sets the level according to the information the supplier will handle:

Information the supplier will handle	Minimum required status
FCI only (no CUI)	Level 1 (Self)
CUI	Level 2 (Self)
CUI, where the prime contract requires Level 2 (C3PAO)	Level 2 (C3PAO)
CUI, where the prime contract requires Level 3 (DIBCAC)	Level 2 (C3PAO)

A small finishing shop that never sees the contract and never reads the statement of work, yet receives a production drawing marked CUI//SP-CTI, or carrying a Distribution Statement B through F because it holds controlled technical information, is handling CUI. Controlled technical information is a category of CUI, and under DoDI 5230.24 it is marked with a Distribution Statement B through F. That statement is among the clearest signals that a drawing should be treated as controlled, absent a determination otherwise by the controlling DoD office. The drawing sets the required level, and the shop's size and its distance from the government customer do not lower that requirement.

Beyond the level itself, the rule attaches obligations that continue after the award. Each supplier handling CUI must reach the required Level 2 status and keep it current. A self-assessed supplier records its results and its affirmation in the Supplier Performance Risk System. A supplier assessed by a C3PAO has its results submitted through the CMMC assessment system, with the affirmation of continuous compliance recorded by an affirming official. The status is not permanent in either case. It must be affirmed on a recurring basis and can lapse. A conditional Level 2 status, granted when a supplier meets the threshold but carries open items, requires an assessment score of at least 88 and the closure of every open item within 180 days. These are not events that happen once at award. They are recurring conditions that a supplier can fall out of at any time.

The Consequence Stays With the Prime

Sending a notice does not move the consequence of a gap onto the supplier. The consequence remains with the prime through three mechanisms.

The first is award eligibility. Where DFARS 252.204-7021 applies, a prime may not let FCI or CUI be processed, stored, or transmitted on a supplier system that lacks the required CMMC status, and before awarding a covered subcontract it must confirm the supplier holds the current status appropriate to the information being flowed down. A supplier notice does not satisfy that requirement. A supplier that loses or never obtains its status becomes ineligible for the work, which leaves the prime with the option to delay the work, source it elsewhere, or proceed in violation of its own contract.

The second is affirmation and status maintenance. The prime must keep its own CMMC status current and affirm its continued compliance each year, and DFARS 252.204-7021 separately requires it to ensure that covered subcontractors hold current status and complete their own affirmations. A prime that cannot show evidence behind those subcontractor controls has made a representation it may be unable to support.

The third is liability under the False Claims Act. The Department of Justice has pursued cybersecurity misrepresentation as civil fraud through its Civil Cyber-Fraud Initiative. A prime that represents supply chain compliance it cannot substantiate, or that knowingly directs CUI to a supplier without the required status, can face that liability. The exposure does not depend on an actual breach. What creates the risk is a representation about cybersecurity compliance that is materially false, made knowingly or with reckless disregard, and connected to payment, award eligibility, or contract performance. In 2025, Raytheon, RTX, and Nightwing agreed to pay $8.4 million to resolve such allegations across 29 DoD contracts and subcontracts, in a matter brought by a former engineer under the qui tam provisions.

The common thread is that the prime answers for the chain it assembled. The regulation distributes the obligation downward through contract language, but the consequences of a failure anywhere in the chain return to the prime that holds the government contract, makes the affirmation, and bears the eligibility and fraud exposure. A notice changes none of that.

Where Controlled Information Actually Goes

A map of how controlled information moves through a supply chain does not resemble an organization chart. It follows the part. A prime receives a contract to deliver an assembly. The assembly requires a machined component. The component requires raw material cut to a specification, machining to a controlled drawing, a heat treatment to a process specification, a surface finish such as anodize or chemical conversion coating, a protective plating, a qualified primer or paint, and a nondestructive test to confirm the

result. Each of those operations is performed by a different company, and several are handled by small shops that specialize in a single process.

The controlled information moves with the part. The machine shop receives the drawing and, in many cases, a tool path or G-code generated from a model based on government technical data. Where that derivative still carries the geometry, tolerances, and process detail needed to produce the controlled part, it remains controlled. The control does not disappear simply because the data has changed form from a model into machine instructions. The finishing shops receive the drawing or the relevant sheet so that they can read the callouts for their operation. The test lab receives the specification it must test against. By the time a part is complete, the controlled drawing and its derivatives have passed through five or six companies, most of which the prime has never directly qualified and may not be able to name.

These lower-tier processors share a profile. They are small. They run lean. Many were selected decades ago for the quality of their process and the reliability of their schedule, not for the maturity of their information systems. A plating shop that has held a Nadcap accreditation for thirty years may operate with a single office computer, an email account, and no written understanding that the drawing in its inbox is controlled. That shop is handling CUI. Under 170.23, Level 2 is required. And it is the tier the prime can see least, and the tier a notice is least able to reach.

Why Notices Are Not a Strategy

The notice approach fails for a structural reason. It treats CMMC compliance as something a supplier will take care of once it has been told to, when compliance is a status that must be verified, sustained, and, in many cases, actively supported. Several specific failures follow.

A notice confirms nothing. A letter that instructs a supplier to reach Level 2 does not establish that the supplier has done so. A returned questionnaire records what the supplier says about itself on the day it answered. Neither produces the current, evidenced status that the regulation requires the prime to rely on before controlled information moves.

A confirmed status goes stale. Even where a prime verifies status at the start, a supplier that held a valid Level 2 self-assessment can let an open item lapse, change the scope of its assessed environment, or pass the point at which its affirmation was due. A verification performed once and never revisited is a photograph of a moving object.

Visibility ends at the first tier. A prime sends its notices to the suppliers it buys from. It rarely reaches the suppliers that those suppliers buy from, yet the regulation

requires compliance at tiers that the prime never contracts with directly. A notice cannot find the plating shop that the prime cannot name.

A requirement without support does not close the gap. This is the failure that notices make most visible. Many of the suppliers that handle controlled information are small shops selected for the quality of their processes, not for the maturity of their information systems. Told to reach Level 2, a number of them do not know where to begin, cannot spare the staff, and have no in-house person who can read NIST Special Publication 800-171 and translate it into their environment. A notice instructs these suppliers to solve a problem they lack the means to address. The requirement is now on record, the shop is still not compliant, and the controlled drawing still arrives in its inbox. Monitoring will detect this gap. Only assistance will close it.

Ownership is diffuse. Procurement sends the notice. Quality owns the supplier's process approval. Security owns the prime's own environment. No single group owns the question of whether a third-tier finishing shop holds a current CMMC status and, if it does not, what the prime intends to do about it.

These are not failures of diligence by individual buyers or engineers. They are the predictable result of treating a continuing obligation as a one-time message.

A Strategic Monitoring and Assistance Function

The answer is to treat CMMC across the subcontractor base the way a defense manufacturer already treats two other obligations that cut across the business: supplier quality and trade compliance. Neither is left to a notice. Each has a defined function, staff with the right training, a documented process, and the authority to stop a transaction that does not meet the standard. CMMC across the subcontractor base needs the same structure to do two jobs: monitor and assist.

The function described here does not perform assessments or certify suppliers. Those roles belong to the suppliers themselves and to accredited third-party assessors. The function manages the prime's own obligation to know where controlled information goes, to confirm that each supplier holding it meets the required level, and to help the suppliers that cannot get there alone.

The monitoring responsibilities answer one question on an ongoing basis: across every tier that handles controlled information, which suppliers hold the required status and which do not.

Data mapping. The function maintains a living map of which suppliers receive FCI or CUI and what they receive. The map follows the controlled drawing and its derivatives through every operation required to build the part, identifying the finishing shops, heat-treat shops, and test labs that procurement records may never have flagged. The

map is the foundation for everything else because the required level for each supplier depends on the data the supplier handles.

Level determination. For each supplier on the map, the function determines the required CMMC level and assessment type using the test in 170.23. A supplier that handles FCI only requires Level 1. A supplier that handles CUI must be at least Level 2, and if the prime contract calls for a third-party assessment, the supplier must hold third-party assessed status as well.

Verification before award. Before any subcontract or purchase order that will move controlled information is awarded, the function confirms that the supplier holds the required status through a current record, a Supplier Performance Risk System status or an assessment result, rather than a returned questionnaire or a signature on a notice.

Flowdown clause management. The function maintains the correct contractual language for each tier and confirms that the requirement to flow down further is present in every subcontract that transmits controlled information. The obligation to cascade is only as strong as the clause that carries it.

Continuous monitoring. The function tracks the conditions that change after the award. It records when each supplier's annual affirmation is due, when a conditional status must convert to final, and when an assessment is set to expire, and it revisits status on a defined cadence rather than waiting for a problem to surface.

Recordkeeping. The function retains the evidence that supports the prime's own affirmation: the data map, the verification records, the clause history, and the monitoring log. This record is what allows the prime to support its CMMC contract compliance with evidence, including its own status maintenance and its obligation to ensure that covered subcontractors keep current status and affirmations.

The monitoring responsibilities tell the prime where the gaps are. The assistance responsibilities are how the prime closes them. A prime that only monitors will produce an accurate list of suppliers it cannot use, while the work those suppliers perform must still be done. Assistance is what keeps a qualified supplier in the chain instead of losing it.

Triage. Not every supplier needs the same help. The function sorts suppliers by two measures: how essential the supplier is to current programs, and how far the supplier is from the status it must hold. A sole-source finishing shop that is far from Level 2 is a different problem from a commodity supplier that is nearly there, and the prime's effort reflects that difference.

Practical enablement. For the suppliers that cannot self-perform, assistance means concrete help: translating the requirements of NIST Special Publication 800-171 into the

supplier's actual environment, providing templates and reference material, offering shared or sponsored tooling where it makes sense, and guiding the supplier through remediation toward an assessable state. Many small shops do not need to be told what the standard is. They need help applying it to the single office network they actually run.

Sourcing expertise. Few primes hold enough internal readiness capacity to support a base of dozens or hundreds of small suppliers. Where that capacity does not exist inside the company, the function arranges it through qualified readiness specialists engaged for the purpose, so that the assistance offered is real rather than a referral to a list of vendors.

Lapse response. When a supplier falls out of status, the function follows a defined response that pairs monitoring with assistance: hold the flow of controlled information, escalate to the program, and work the supplier back into status or, where that is not possible, identify and qualify an alternate source. A lapse handled through an established process is a manageable event. A lapse discovered during an audit is not.

The function should also work to reduce how much controlled information moves down the chain in the first place. For each supplier, the question is what that supplier actually needs to perform its operation. A finishing shop may need a single sheet and a callout rather than a full model, and a process step may be supportable through a controlled extract or prime-managed access rather than a full drawing package released into the supplier's own systems. Information that never reaches a supplier system does not have to be protected there. Reducing unnecessary flow is often the most effective control of all, and it lowers the number of suppliers that must carry a higher status.

Placing and Staffing the Function

A function with these responsibilities needs a home, a defined staff, and real authority. Several placements work, and the right one depends on the organization.

In many manufacturers, the natural home is alongside supplier quality. Supplier quality already maintains an approved supplier list, audits and reapproves suppliers on a cadence, and has the authority to remove a supplier that falls below standard. Adding a CMMC status to the data that those teams already track and a CMMC gate to the approval they already perform extends the existing structure rather than building a new one.

In organizations with a mature trade compliance group, that group is a strong alternative. Trade compliance already reasons about which technical data may go to which party under export rules, which is close to the question CMMC asks about which controlled information may go to which supplier. The two analyses are not identical, but the discipline transfers.

Wherever it sits, the function needs to combine four capabilities. It needs people who understand both the regulation and the manufacturing process, because a person who can read 170.23 but cannot recognize that a plating drawing carries CUI will map the chain incorrectly. It needs integration with the systems the company already runs, the enterprise resource planning supplier master, the quality system, and the contract management system, so that CMMC status lives beside the other facts the company keeps about a supplier. It needs the capacity to assist, whether through internal readiness staff or through specialists engaged for the purpose, so that a supplier found short of the standard can be helped rather than simply dropped. And it needs the authority to hold a transaction, the same authority that supplier quality holds when a process falls out of control, so that the verification gate is a real gate and not a formality.

Building the Function in Sequence

A prime does not need to stand up a fully staffed department before it can begin. The function can be built in a sequence that delivers protection at each step.

The first step is to map the chain for the programs that carry the most controlled information. This produces the supplier and data map for the work that matters most, and it reveals the lower-tier processors that current records miss.

The second step is to classify each mapped supplier by required level and verify the current status of suppliers already handling controlled information. This converts the map into a clear list of who holds the required status, who does not, and where the gaps sit.

The third step is to triage those gaps and begin assistance where it matters most, with the suppliers that are both essential to current programs and furthest from the status they must hold. This is the step that keeps qualified suppliers in the chain rather than losing them as deadlines arrive.

The fourth step is to build the verification gate into the procurement and supplier approval process, so that no new flow of controlled information begins without a status check. From that point forward, the chain stops accumulating new gaps.

The fifth step is to establish the monitoring cadence, the calendar of affirmations, conversions, and expirations, so that the verified status of the chain stays current rather than degrading after the initial effort.

Each step stands on its own. A prime that completes only the first three is in a far better position than one that has sent notices and filed the replies. A prime that completes all five has replaced a stack of notices with a managed capability.

Conclusion

The regulation has settled the question of scope. CMMC compliance is required at all tiers of the defense supply chain; the required level follows the controlled information rather than the position in the chain, and the conditions that establish compliance continue after award and can lapse at any time. The smallest finishing and testing shops handle controlled information as a normal part of their work, and they are the tier that notices reach least, and the prime can verify least.

A prime that sends a notice and files the reply has not met this obligation. It has recorded an instruction and left the substance unmanaged. Meeting the obligation requires a function that monitors compliance status across every tier that handles controlled information and, in the same motion, assists suppliers that cannot reach or maintain that status on their own. Monitoring identifies the suppliers a prime is about to lose, and assistance is what keeps them. Neither does the job by itself.

That function is how a prime maintains the evidence behind its CMMC contract compliance, keeps its programs eligible, and answers for the chain it has assembled. A prime that builds it has replaced a notice with a strategy.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced who advises Defense Industrial Base contractors and the attorneys who counsel them on CMMC Level 2 readiness, enablement, and implementation. He is the author of The CMMC Decision, Second Edition, an Associate Member of the American Bar Association Section of Public Contract Law, and a professional member of ISACA. His work is grounded in more than thirty years of experience in information technology and cybersecurity, including direct experience with aerospace manufacturing environments, controlled machining workflows, and enterprise resource planning systems, as addressed in this paper.

David can be reached at dkoran@davidkoran.com or (802) 335-2662.

References

32 CFR Part 170, Cybersecurity Maturity Model Certification (CMMC) Program. Published October 15, 2024; effective December 16, 2024.

32 CFR 170.23, Application to Subcontractors.

32 CFR 170.21, CMMC Status Requirements (conditional status and score threshold).

32 CFR 170.17, CMMC Level 2 Certification Assessment and Affirmation Requirements.

32 CFR 170.22, Affirmation.

Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), final rule. Published September 10, 2025; effective November 10, 2025.

DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement.

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

NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

DoD Instruction 5230.24, Distribution Statements on DoD Technical Information.

DoD Instruction 5200.48, Controlled Unclassified Information (CUI).

U.S. Department of Justice, settlement with Raytheon Company, RTX Corporation, and Nightwing Group (2025), resolving False Claims Act allegations of cybersecurity noncompliance across DoD contracts and subcontracts.