LAWFARE

Courts & Litigation Cybersecurity & Tech Executive Branch

Rulemaking by Memo: Why CMMC Suspension Deserves Review

Michael McLaughlin, Harvey Rishikof

Wednesday, September 9, 2026, 10:35 AM

DOD CIO suspended the backbone of defense supply-chain security with a memo. Under new case law, it may not survive the courts—or the threat.

On July 13, the Department of Defense suspended the central mechanism it had spent more than five years building to secure the defense industrial base (DIB). Two memoranda, one from the department's chief information officer (CIO) and one from the under secretary of defense for acquisition and sustainment, paused the November 2026 transition to phase two of the Cybersecurity Maturity Model Certification (CMMC) Program, directed contracting activities to accept only self-assessment, ordered higher-tier assessment requirements stripped from active solicitations and existing contracts, and barred waivers during a 60-day review.

The department frames the suspension as relief from bureaucratic burdens on small businesses. That concern is not frivolous. But the manner of the action, the security judgment it reflects, and the factual premises on which it rests all deserve closer scrutiny than the memoranda and a press conference allow. Two recent shifts in administrative law make the manner especially consequential. The Supreme Court has stripped agencies of the interpretive deference that once cushioned actions like this one, and the Court has tightened the rules governing how an agency may change course.

Measured against that landscape, the suspension may be legally fragile in several separate respects. Measured against the cyber threat environment, it trades a real security benefit for a burden reduction smaller than advertised. And measured against the available data, its central factual premise does not hold.

The Instrument and the Reasoning

CMMC does not rest on a memorandum. It rests on two legislative rules adopted through a public notice-and-comment period. The CMMC Program rule, which took effect in December 2024, establishes the program's assessment levels, the

third-party assessor ecosystem, the annual affirmation regime, and a case-by-case waiver authority vested in senior service and component acquisition officials.

The companion acquisition rule, effective Nov. 10, 2025, added the operative contract clause and its solicitation provision to the Defense Federal Acquisition Regulation Supplement (DFARS). In other words, the CMMC Program rule defines the structural standards, assessment levels, and compliance criteria, and the acquisition rule operationalizes those standards into mandatory contract clauses and procurement procedures. Both rules carry the force of law. Both remain on the books today. Neither has been amended or rescinded.

A Guidance Document Cannot Suspend a Binding Rule

The line between a legislative rule and an interpretive one is the spine of this problem. Under the Administrative Procedure Act, an agency may change an interpretive rule—its reading of what an existing regulation means—quickly and without public process; the Supreme Court confirmed as much in *Perez v. Mortgage Bankers Association* (2015), which held that agencies need not use notice-and-comment to revise an interpretation. But *Perez* reaffirmed the other legislative factor in the same breath: A legislative rule, one that carries the force of law and sets substantive obligations, can be amended or repealed only through the same notice-and-comment process that created it.

The dispositive question, then, is not how fast the department moved but what kind of change it made. If the memoranda merely adjust the pace of a phase-in period the rule already contemplates, the changes are on solid ground. If the memoranda instead alter the operative legal obligations the rule imposes, the Administrative Procedure Act requires the department to proceed with a notice-and-comment period: the same public process that forces an agency to expose its reasoning to testing and to build a record a court can review. At present, both the department and the memoranda are silent as to whether this is a pace adjustment or an alteration of the legal obligations.

The Pentagon's best defense is that it has discretion over its own rules. The program rule builds in a phased implementation schedule, and contracting activities retain latitude over which assessment level a given procurement requires. On that reading, pausing the transition to a future phase is an exercise of retained discretion, not an amendment of the rule. As to the timing of the phase-in period, that argument has real force, and any honest analysis should concede it. An agency that built a phased schedule into its rule may generally adjust the pace at which it climbs that schedule.

The difficulty is that the memoranda appear to go well beyond adjusting a pace. They direct the affirmative removal of existing requirements, instructing contracting officers to amend active solicitations that contain obligations for

review by a Certified Third-Party Assessor Organization or Defense Industrial Base Cybersecurity Assessment Center and to strike those obligations from awarded contracts at the next modification or option. The Pentagon could use its discretion to decline to add a requirement to a future procurement. Directing the removal of requirements already imposed under a rule that remains in force is something else.

The Pentagon will characterize all of this as implementation discretion the rule itself confers. With pacing, that characterization holds. But two features argue against this view for the department. Stripping substantive obligations from contracts that already contain them changes the operative legal content that the rule imposes, not merely the timing of its phase-in period; and a categorical bar on waivers refuses to exercise a discretionary authority that the rule expressly grants.

Once the action is understood as a substantive change to a legislative rule rather than a reading of it, the Administrative Procedure Act supplies the constraint: Such a change requires a public notice-and-comment opportunity. That leaves the department a choice with no comfortable exit. If the memoranda are mere guidance, they cannot lawfully accomplish a substantive suspension of the rule's operation. If they are substantive rules, they were issued without the required public process and without invoking the narrow "good cause" exception that alone would excuse skipping it, which makes them potentially procedurally vulnerable on their face.

An Agency That Changes Course Must Give Reasons

Even assuming the Department of Defense had the authority to act, an agency that reverses course must explain itself. The governing line runs from *Motor Vehicle Manufacturers Association v. State Farm* (1983), which requires an agency to examine the relevant data and draw a rational connection between the facts it finds and the choice made. It continues through *Federal Communications Commission v. Fox Television* (2009) and *Encino Motorcars v. Navarro* (2016), which require an agency reversing position to acknowledge that it is doing so and to give a reasoned explanation for it. The precedent culminates in *Department of Homeland Security v. Regents* (2020), which further requires the agency to weigh the serious reliance interests its prior policy created.

The Supreme Court restated this framework in 2025 in *Food and Drug Administration (FDA) v. Wages and White Lion Investments*. The Court there sided with the FDA, but the reason it did so is what matters here: It found the agency's earlier guidance too tentative and caveat-laden to have established a definitive prior position, so there was no clear "change" the agency had to justify. Along the way, the Court confirmed the controlling test: An agency may change an existing policy only if it provides a reasoned explanation, acknowledges that it is changing its position, and considers serious reliance interests.

The CMMC suspension differs from the facts that saved the FDA in the way that matters. The department's prior position was not a set of tentative hints; it was a codified rule and a published implementation schedule. The reversal to self-assessment is therefore an unmistakable change of position, and neither memorandum acknowledges it as such. Nor has the Pentagon explained the need to shift away from the program's premise—that self-attestation did not reliably reflect contractor security. Under *Wages and White Lion*'s own test, that is the kind of unexplained reversal the doctrine is meant to catch.

Lower courts are applying this framework to reversals executed without a reasoned record. In *State of New York v. Kennedy* (2025), a federal district court held that agency action announced by press release, which had disrupted settled reliance without an articulated rationale, was arbitrary and capricious. A suspension announced by a same-day memorandum, silent on the risk it creates and the reliance it upends, invites the same analysis. The point is narrow and worth stating precisely: This kind of review polices the agency's reason-giving, not the wisdom of its policy choice. A political motive is permissible; an absent rationale is not. The memoranda do not fail because pausing CMMC is necessarily bad policy. They fail because they do not show the work or the policy reasons why.

The reliance interests here are neither speculative nor marginal. They include a third-party assessor ecosystem that the Defense Department itself accredited, and the contractors and service providers that invested substantial amounts in readiness on the strength of the published implementation date of November 2026. The memoranda do not acknowledge those interests, let alone weigh them. Under *Regents* and *Wages and White Lion*, that silence appears to be a defect.

Statutory Authority and the Limits of Discretion

The second question is whether the suspension stays within the authority Congress granted. Here, the terrain shifted in 2024. In *Loper Bright Enterprises v. Raimondo*, the Supreme Court overruled *Chevron v. Natural Resources Defense Council* and held that courts must use their own independent judgment in deciding whether an agency has acted within its statutory authority, rather than deferring to the agency's reading of an ambiguous statute. For CMMC, this cuts two ways.

On one side, *Loper Bright* does not endanger the CMMC rules themselves; the Supreme Court was explicit that the mere fact that a rule once relied on *Chevron* is not a reason to reopen it, so the program's underlying rules are secure. On the other side, and decisively here, the Defense Department earns no deference for its view that the statute directing it to build a DIB cybersecurity framework, and its own rules, permit suspending the framework's verification core by memorandum. A reviewing court decides that question for itself. The governing statute directs the secretary to develop a consistent, comprehensive framework to enhance that

cybersecurity. Under this reading, whether authority to develop and maintain a framework includes authority to suspend the framework's central mechanism is now a question for a court, not a matter of agency latitude.

The emerging case law supplies the method. Courts are not sweeping away agency action across the board; where a statute genuinely delegates authority, they respect the delegation. The U.S. Court of Appeals for the Federal Circuit's en banc decision in *Lesko v. United States* (2025) offered the now-standard road map: Confirm the breadth of the delegation first, and then ask whether the challenged action merely fills a gap within it or goes further.

The U.S. Court of Appeals for the District of Columbia Circuit likewise upheld agency action within a genuine delegation in *Solar Energy Industries Association v. the Federal Energy Regulatory Commission* (2025). But the same independent review has invalidated action a court reads the statute to forbid: The U.S. Court of Appeals for the Fifth Circuit vacated a Labor Department rule in *Restaurant Law Center v. Department of Labor* (2024) that had survived under *Chevron*. The suspension's vulnerability sits at the second step of that road map. A directive that strips out a verification requirement the framework was built to impose is readily characterized as going further than filling a gap.

The Categorical Waiver Bar Is the Cleanest Defect

One feature of the memoranda does not require a court to resolve any of the harder questions raised by this analysis. The program rule vests waiver authority in senior service and component acquisition officials to be exercised case by case. The CIO's memorandum directs that no waivers be granted during the review. A blanket instruction that no official may exercise a discretionary authority that the rule confers is not an exercise of that discretion; it is a refusal to exercise it at all, in direct tension with the rule's text. This objection turns on nothing more than a comparison between the memorandum's categorical command and the regulation's plain terms, which is why it is the cleanest of the defects and the hardest for the Department of Defense to answer.

To the extent the suspension can be recast as a decision not to enforce the higher-tier requirements, it borrows traits from the presumption against judicial review of nonenforcement recognized in *Heckler v. Chaney* (1985). But *Chaney* protects an agency's decision to stay its hand; it does not protect affirmative commands to modify existing contracts or a categorical refusal to waive the power the rule confers. The department's strongest move is forward-looking: If it follows the review with genuine notice-and-comment rulemaking, much of the procedural objection dissolves going forward. The objection developed here is to what the department has done now, and for the interim, outside that process.

The Adversary the Memoranda Do Not Mention

CMMC exists for a reason. For more than a decade, the DIB has been a preferred target of state-sponsored cyber espionage, and contractor self-reports to the controls in the applicable federal cybersecurity standard did not reliably reflect reality. We argued in 2022 that reliance on the DFARS and National Institute of Standards and Technology standards alone had proved insufficient to defend the DIB, noting industry assessments in which not a single company reviewed was fully compliant. We urged the government to lean harder on verified, accredited security rather than self-reporting.

CMMC's third-party assessment requirement was the government's answer to precisely that verification gap. Contractors attested to controls they had not implemented. The result was that controlled unclassified information bled to U.S. adversaries, including critical development data, technical specifications, and program timelines. The suspension now reverses that answer and returns the DIB to the self-attestation model whose inadequacy was documented years ago.

That threat has not receded. Russian state-sponsored actors have maintained persistent, months-long access to defense contractor networks, exfiltrating development timelines and specific military technologies. Chinese government-linked groups have systematically targeted the base for blueprints, proprietary research, and technical data illuminating U.S. military capabilities. In April 2026, the Cybersecurity and Infrastructure Security Agency and allied cyber authorities warned that Chinese state-sponsored operations have industrialized, fusing the country's intelligence, military, and civilian security services into a single continuous exfiltration enterprise. These adversaries are not observing a 60-day review.

Against that backdrop, the most striking feature of the two memoranda is what they omit. Across their combined text, they discuss barriers, burden, red tape, and DIB expansion. They do not mention China. They do not mention Russia. They do not mention exfiltration, espionage, or the theft of military technology, though those are the precise harms the program was built to prevent. A decision that accounts for the cost of compliance fully and not at all for the cost of compromise to our warfighters is not a balanced weighing of equities. It is a weighing with one side of the scale left empty, and that omission is not only a policy concern but a marker of the reasoned decision-making defect that the law polices.

The point is not that suspending phase two will cause a specific breach; causation in this domain is rarely so clean. The point is firmer. Reverting to self-assessment does not lighten the security obligations of contractors handling controlled unclassified information; it removes the independent check that those obligations are met, for precisely the population whose self-reports have proved least reliable. The department has not made the DIB more secure. It has made the insecurity harder to see.

The Numbers Do Not Support the Premise

The suspension's central factual justification is capacity—that the assessor ecosystem is too small to certify the DIB on any reasonable timeline. The Department of Defense has characterized the mismatch as roughly 100,000 companies requiring assessment against roughly 100 available assessors. That framing does not match the ecosystem's own data.

Drawing on the monthly counts reported at the CMMC accreditation body's town halls from November 2025 through June 2026, monthly new level two certifications rose steadily from 123 to 279. Even assuming assessors operate at only half their available capacity, monthly throughput climbed above 400 assessments ahead of demand. Had that conservative capacity been fully used since November 2025, the ecosystem could have produced roughly 2,939 level two certifications; it produced 1,666. The difference, more than 1,200 certifications, does not describe a shortage of assessors. It describes unused capacity.

The record also undercuts the premise that the phased rollout was failing. In the analysis accompanying the program rule, the department projected that roughly 500 companies would certify in the first year of phase one. By June 2026, roughly five times the estimated level two assessments had been completed. A significant driver has been the emergence of certified managed service providers delivering compliant solutions at scale to smaller suppliers. This is the exact capacity that the department wrongly assumes does not exist in its reasoning for a capacity-based suspension.

The cost figures deserve the same scrutiny. The Small Business Administration (SBA), endorsing the suspension, estimated the total compliance cost for a small contractor requiring third-party assessment at roughly $593,800. But the SBA's own analysis estimates the cost for a firm eligible for self-assessment at roughly $388,600. By the government's own accounting, roughly $388,600 of the burden is owed regardless of whether an independent assessor is ever involved, because it is the cost of implementing the security controls that federal acquisition rules have required for years and that the memoranda leave in force.

Pausing phase two does not relieve that cost. It defers only the incremental third-party assessment, the smaller share of the SBA's own figures, while removing the government's ability to confirm the larger share was ever spent. We contend that, for wide adoption, some tax benefits or write-offs would be helpful for the business community.

The Right Problem, the Wrong Instrument

The concern animating the suspension is legitimate. Compliance costs fall hardest on small firms, assessor-scheduling frictions are real, and an industrial base that sheds its smallest suppliers is a national security problem itself. A serious response might expand assessor capacity, subsidize small-business readiness, leverage managed service providers, or tier requirements more granularly. Each of those tools works within the rule and preserves the verification the rule exists to provide, and each could be pursued through a proposed rule, with any interim measure supported by a genuine good-cause showing, rather than by same-day guidance.

What the Pentagon chose instead was the instrument that maximizes its legal exposure across every doctrine canvassed above: a same-day suspension that unwinds the operation of a legislative rule without rulemaking, refuses to exercise the rule's own safety valve, reverts to a policy the program was built to reject without engaging that premise, and proceeds without a reasoned record or any accounting of the threat. After *Loper Bright* and *Wages and White Lion*, that is not a technicality. It is the ground on which such an action is tested.

The timing also sits awkwardly against the administration's own cyber posture. Two days after the CMMC suspension, the White House announced "Gold Eagle," a voluntary public-private clearinghouse to identify and patch software vulnerabilities at the speed the era of artificial intelligence demands, an initiative that treats coordinated, centralized verification across government and industry as a national security imperative.

As one participating executive put it in an interview with the Washington Post, the country has "one national attack surface, and it doesn't care about public versus private." That premise is difficult to reconcile with the one underlying the CMMC pause. The same government that is building new machinery to verify and harden the private-sector attack surface is, in the same month, removing the mechanism that verifies the defense industrial base, the segment of that surface adversaries target most. Whatever the merits of each program in isolation, the two moves point in opposite directions on the same question: whether verification is a burden to be lifted or a defense to be maintained.

A note on remedy: The Supreme Court's decision in *Trump v. CASA* (2025) narrowed the availability of nationwide injunctions and cast doubt on how far a court may go in setting aside an agency action, while *Corner Post v. Board of Governors* (2024) widened who may sue and when, holding that the clock on a challenge runs from the plaintiff's injury rather than from the rule's adoption. The combined effect is a litigation landscape that is easier to enter and harder to resolve cleanly. Newly injured assessors and suppliers will have standing and a

fresh filing window, but a court that finds the suspension unlawful may grant relief only to the parties before it rather than setting the memoranda aside for everyone. That uncertainty is why the more consequential check may not be judicial at all.

The statute that produced CMMC came from Congress, and the review the Defense Department has promised will unfold in public view; whether the interim posture actually preserves the security baseline the department claims is a question the political branches are well positioned to press, and to press faster than scattered litigation could resolve it.

The Department of Defense reached a legitimate concern with the wrong instrument, unwinding two binding rules by same-day memo in the one way that maximizes its legal exposure after *Loper Bright*, *Wages and White Lion*, and *Regents*. The capacity premise offered to justify the suspension conflicts with the ecosystem's own numbers, which show unused assessor capacity rather than a shortage.

What the memoranda actually accomplish is not relief but risk: Reverting to self-attestation strips the independent check on the very contractors whose self-reports have proved least reliable, at the precise moment China and Russia have industrialized their theft of our defense technology. The answer to a real burden was never to abandon verification by memo. It was to do the work the law requires, through notice-and-comment rulemaking and a record that earns the review the political branches and the courts alike should now demand.

Michael McLaughlin

Read More

Michael McLaughlin co-leads the Cybersecurity and Data Privacy practice at Buchanan Ingersoll & Rooney. He served as Senior Counterintelligence Advisor for U.S. Cyber Command and Chief of Counterintelligence and Human Intelligence for the Cyber National Mission Force. Michael co-authored "Battlefield Cyber: How China and Russia Are Undermining Our Democracy and National Security."

Harvey Rishikof

Read More

Harvey Rishikof is a visiting professor for Carnegie Mellon Institute for Strategy & Technology (CMIST) and senior counsel of the American Bar Association Standing Committee on Law and National Security's Advisory Committee.

}