FedRAMP 20x, Certification Classes, and the CMMC Cloud Requirement

What the Consolidated Rules for 2026 Mean for Every Defense Contractor Using the Cloud for CUI

David W. Koran

CyberAB Registered Practitioner Advanced (RPA)

July 2026

On July 4, 2026, the federal government's program for certifying the security of commercial cloud services, known as FedRAMP, opened optional early adoption of a new rulebook, with mandatory adoption for all stakeholders set for January 1, 2027. The Consolidated Rules for 2026 launch a modernized certification path called FedRAMP 20x, retire the familiar Low, Moderate, and High labels in favor of Certification Classes A through D, and establish a single official designation, FedRAMP Certified, for every cloud service the program approves. The public directory of approved services, the FedRAMP Marketplace, will carry the new vocabulary as the transition proceeds, and as of this writing it still displays the familiar impact levels alongside each listing's certification type.

If your company handles Controlled Unclassified Information, or CUI, under Department of Defense contracts, this change reaches your business whether or not anyone on your team follows FedRAMP news. Every cloud service that stores, processes, or transmits your CUI must meet a specific FedRAMP standard, and a certified assessor will verify that during your CMMC assessment. A cloud service that falls short of the standard is a finding, and a finding in this area is not a paperwork problem. It puts the certification itself at risk, and the certification is what keeps the company eligible for the contracts.

Here is the difficulty. The CMMC rule did not move when FedRAMP did. The cloud requirement in 32 CFR Part 170 is still written in terms of FedRAMP Moderate, a label that the program issuing it is now retiring. For the next several years, contractors will be evaluating cloud vendors whose certifications speak one vocabulary against a regulation that speaks another. The translation between the two is manageable, but it has to be done deliberately, because the new vocabulary produces at least one vendor claim that is completely accurate under FedRAMP rules and completely inadequate under the CMMC requirement at the same time.

Why a Cloud Certification Program Appears in a Defense Contract

Some background helps here, because the requirement predates CMMC and is often misunderstood as a CMMC invention. FedRAMP exists so that the federal government does not have to security test the same commercial cloud service dozens of times. A cloud provider undergoes one rigorous independent assessment, the results are certified, and the service appears on the FedRAMP Marketplace where any agency can see its status. The historical labels of Low, Moderate, and High described how much protection the assessment covered, with Moderate serving as the standard for most sensitive but unclassified government data.

In 2016, the Department of Defense extended that logic to its contractors through DFARS clause 252.204-7012, which appears in virtually every defense contract involving CUI. The reasoning was straightforward. If the Department itself would not place this category of data in a cloud service below the Moderate standard, a contractor holding the same data on the government's behalf should not either. The clause therefore requires that any external cloud service used for this data meet security requirements equivalent to the FedRAMP Moderate baseline. For years, that requirement sat in contracts largely unverified. CMMC is the verification mechanism. During a CMMC Level 2 assessment, a CMMC Third Party Assessment Organization, called a C3PAO, examines the contractor's environment, and every cloud service touching CUI is inside the scope of that examination.

What the CMMC Rule Requires for Cloud Services That Handle CUI

Under 32 CFR Part 170, a cloud service that stores, processes, or transmits CUI for a company seeking CMMC Level 2 certification must satisfy one of two conditions. The first path is the simple one: the specific service offering is FedRAMP Authorized at the Moderate baseline or higher and is listed on the FedRAMP Marketplace. The contractor can point to a public government record, and the question is largely settled apart from confirming that the listing covers the actual service and configuration the company uses.

The second path, called equivalency, is for cloud services that never went through the FedRAMP process but claim to meet the same standard. The Department of Defense defined this path in a memorandum dated December 21, 2023, and the definition is demanding. The provider must demonstrate 100 percent compliance with the latest FedRAMP Moderate security control baseline, validated by a Third Party Assessment

Organization, or 3PAO, which is an independent assessment firm recognized by FedRAMP. The similar acronyms invite confusion, and the distinction matters: a 3PAO assesses cloud providers under FedRAMP, while a C3PAO assesses defense contractors under CMMC, and the two operate under separate accreditations. Plans of Action and Milestones, or POA&Ms, which are documented plans to fix a known gap at a later date, are not permitted for any security control; only routine operational items may remain open. The provider must maintain a complete documentation package called the Body of Evidence and produce it on request to the contractor's C3PAO or to DIBCAC, the Department's own assessment arm. The memorandum also states that meeting the equivalency standard does not confer an actual FedRAMP authorization. Both paths, it is worth noting, are defined by name relative to the Moderate baseline.

What Changed at FedRAMP in 2026

FedRAMP announced the 20x initiative in March 2025 with the goal of making cloud certification faster, more automated, and more accessible to commercial providers, and ran it as a pilot through early 2026. On June 25, 2026, the program published the Consolidated Rules for 2026, which opened for optional early adoption on July 4, 2026, took mandatory effect for all stakeholders on January 1, 2027, and govern the program through the end of 2028. The rules replace the Low, Moderate, and High labels with Certification Classes. Under the mapping FedRAMP published, Class B includes the former Low baseline, Class C includes the former Moderate baseline, and Class D includes the former High baseline. Class A is new and has no predecessor among the baselines. FedRAMP made this change for a defensible reason: the old labels were routinely confused with the Department of Defense Impact Level system, which uses similar words to measure different things. The rules also establish FedRAMP Certified as the single official authorization label, while the Marketplace separately identifies each service's certification type, meaning 20x or the legacy process known as Rev5, along with its baseline, with class labels phasing in as the transition proceeds.

The transition dates matter for planning. The Class A pipeline opens on August 3, 2026, and the Class B and Class C pipelines open on August 31, 2026. FedRAMP stops accepting applications for new certifications under the legacy process on June 11, 2027, and nothing in the transition strips any provider of an authorization it already holds. A service that is FedRAMP Moderate Authorized today is exactly as acceptable for CUI tomorrow as it was yesterday. The practical consequence is narrower and quieter than a revocation: the word Moderate will gradually stop appearing on new certifications while remaining the operative word in the regulation that governs CUI in the cloud.

Class A, the Designation Every Contractor Will Start Hearing About

Class A deserves its own explanation because it is where the potential for honest confusion is concentrated. Class A is a transitional designation that FedRAMP deliberately designed as an entry point into the federal market. A provider qualifies on the strength of an existing assessment under an external framework, initially a SOC 2 Type II report, which is a widely respected commercial audit of a company's security controls. The provider then has a window of two years to complete a full FedRAMP assessment and obtain a Class B, C, or D certification. During that window, the service remains in the Preparation phase on the Marketplace. Readers with history in this space can locate Class A quickly by its lineage: FedRAMP Ready, the old designation for providers preparing for full authorization, stops accepting submissions on July 28, 2026, and FedRAMP directs those providers toward Class A certification instead. FedRAMP Ready never satisfied the CMMC cloud requirement, and its successor occupies the same preparatory ground. None of this is a defect in the program. It is a sensible way to bring capable commercial providers toward federal standards, and a provider holding a Class A certification has done nothing wrong by saying so.

The issue is what the statement does and does not establish. Because FedRAMP Certified is now the single official label, a vendor holding a Class A certification can state, with complete accuracy, that its service is FedRAMP Certified. That statement carries no information about the Moderate baseline. Beginning August 3, 2026, when the Class A pipeline opens, a cloud vendor whose only completed independent assessment is a SOC 2 Type II report will be able to describe its service, truthfully, as FedRAMP Certified. A SOC 2 Type II has never satisfied the CMMC cloud requirement for CUI, however strong the security program behind it, because the CMMC requirement is defined against a specific federal baseline rather than against general security quality. Placing a FedRAMP class designation on top of a SOC 2 report does not change that analysis. This is a question of scope, not of anyone's integrity, and executives should expect the phrase FedRAMP Certified to appear in sales conversations long before their compliance teams have internalized what it now covers.

The Equivalency Path Now Has a Measurement Problem

FedRAMP has stated plainly that it does not support or adjudicate equivalency and that questions about how its certifications map to CMMC belong to the Department of Defense. The Department, as of this writing, has not issued guidance connecting the

new certification classes or the 20x assessment model to the CMMC cloud requirement. That silence leaves two open questions of very different sizes.

The Marketplace path is the smaller one. A Class C or Class D certification occupies the position formerly labeled Moderate or High, and FedRAMP's stated position is that any FedRAMP Certification constitutes a FedRAMP authorization for purposes of statutory and regulatory requirements. A contractor relying on a Class C-listed service has a reasonable basis to treat the requirement as met. The prudent move is to document the reasoning in the company's assessment record: the class, the certification type, the exact service offering, and the assessed boundary. The contractor should supply the translation between the old vocabulary and the new one rather than assume an assessor will supply it on the company's behalf.

The equivalency path is the larger question. The December 2023 memorandum defines equivalency as 100 percent compliance with the FedRAMP Moderate security control baseline, which is a specific list of several hundred individual security controls. The 20x assessment model is organized differently, around a streamlined set of measures called Key Security Indicators that rely on automated, machine-readable evidence rather than a control-by-control audit. Both approaches aim at security, but they do not measure in the same units. A provider that has produced 20x evidence but holds no certification cannot map that evidence onto the memorandum's requirement, because there is no published crosswalk between the two. Until the Department speaks, the memorandum means exactly what it says: the control baseline, an independent 3PAO assessment, closed POA&Ms, and a complete Body of Evidence. A provider offering 20x participation as a substitute for that package is offering something the memorandum does not recognize.

Reading Vendor Claims Against the Requirement

The table below summarizes how the claims a contractor is likely to hear over the next year map onto the requirement as it stands today. The left column is what appears in the proposal or the sales deck. The right column is what a compliance team, or an assessor, should conclude from it.

What the vendor says	What it means under the CMMC requirement
FedRAMP Moderate Authorized under the legacy process and listed on the FedRAMP Marketplace	Meets the requirement, provided the specific service offering and the assessed boundary match the way your company will actually use the service for CUI.
FedRAMP High Authorized or Class D Certified, listed on the Marketplace	Meets the requirement, subject to the same service offering and boundary verification.
Class C Certified, listed on the Marketplace	Class C occupies the position formerly labeled Moderate. This is a defensible basis for use, but the company should record the class, the certification type, the exact offering, and the boundary in its assessment documentation rather than assume the mapping is self-evident.
Class A or Class B Certified	Does not meet the requirement. Class B corresponds to the former Low baseline. Class A is a transitional designation built on an external framework such as SOC 2 Type II.
FedRAMP Certified, with no class stated	Not enough information to conclude anything. Ask for the class and the specific service offering.
FedRAMP 20x, with no class or Marketplace listing	Not enough information to conclude anything. Participation in the 20x process is not a certification.
FedRAMP equivalent, without an independent 3PAO assessment, closed POA&Ms, and a Body of Evidence	Does not meet the requirement as defined by the Department of Defense in December 2023.
SOC 2 Type II, ISO 27001, or general commercial security claims	Does not meet the requirement for cloud services that store, process, or transmit CUI, regardless of how strong the underlying security program may be.

What This Analysis Does Not Say

Because this subject touches the marketing of a large industry, precision about the boundaries of the argument matters. Nothing here suggests that FedRAMP 20x is a weaker program than its predecessor; in several respects its continuous monitoring model is more demanding than the periodic reporting it replaces. Nothing here suggests that the Department of Defense has rejected the new classes; the Department has simply not yet addressed them. Nothing here questions the status of providers who hold FedRAMP Moderate or High authorizations today; those authorizations remain fully valid through the transition. And nothing here accuses Class A providers of misrepresentation; the label is FedRAMP's own, used exactly as FedRAMP intends. The argument is narrower. Two government programs currently describe the same subject in

different vocabularies, the regulation binding the contractor is written in the older one, and under both the DFARS clause and the CMMC rule it is the contractor, not the cloud provider, who carries the burden of verifying that the standard is met.

The Questions That Protect the Company

An executive does not need to master the control baselines to manage this exposure. Five questions, asked of the compliance team and answered in writing, cover the ground. First, which cloud services in our environment store, process, or transmit CUI, including services embedded inside other services? Second, for each one, what is the exact service offering name and its current status on the FedRAMP Marketplace, stated by class or by legacy baseline, and is it certified or merely in the Preparation phase? Third, for any vendor relying on equivalency rather than a Marketplace listing, has our team actually examined the Body of Evidence and confirmed that no security control POA&Ms remain open? Fourth, does the assessed boundary of each certification cover the specific components and configuration we use, since certifications attach to defined offerings rather than to company names? Fifth, is all of this recorded in our System Security Plan, so the answer exists in our documentation before an assessor asks the question?

The last point deserves emphasis because of how the consequence arrives. There will be no announcement and no deadline. The question surfaces during a C3PAO assessment as an ordinary document request, when the assessor asks which cloud services handle CUI and what the FedRAMP status of each one is. At that moment, the answer is either in the Marketplace record or in the Body of Evidence, or the company has a finding midway through the assessment it has spent months preparing for. The Consolidated Rules for 2026 leave the CMMC cloud requirement exactly where it was while changing the language vendors will use to describe themselves, and the companies that navigate the change well will be the ones that treat every FedRAMP claim as a question about a specific service offering, a specific class, and a specific evidence package. That was already the correct practice before July 4. The new vocabulary only raises the cost of skipping it.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced (RPA). He advises Defense Industrial Base contractors and the legal counsel who represent them on complex CMMC Level 2 readiness, enablement, and implementation. He is an Associate Member of the American Bar Association Section of Public Contract Law and the author

of The CMMC Decision, and his commentary has appeared in National Defense Magazine. He can be reached at dkoran@davidkoran.com and (802) 335-2662.

References

32 CFR Part 170, Cybersecurity Maturity Model Certification (CMMC) Program. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

Department of Defense Chief Information Officer, Federal Risk and Authorization Management Program Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings, December 21, 2023. https://dodcio.defense.gov/Portals/0/Documents/CMMC/FedRAMP-AuthorizationEquivalency.pdf

FedRAMP, Propelling Change: FedRAMP Launches Consolidated Rules for 2026, June 25, 2026. https://www.fedramp.gov/2026-06-25-propelling-change-fedramp-launches-consolidated-rules-for-2026/

FedRAMP, Notice NTC-004, Initial Outcome from RFC-0020 FedRAMP Authorization Designations. https://www.fedramp.gov/notices/0004/

FedRAMP Consolidated Rules for 2026, Important Dates. https://www.fedramp.gov/2026/timeline/

FedRAMP Marketplace. https://www.fedramp.gov/marketplace/products/

FedRAMP Consolidated Rules for 2026, FedRAMP Certification Classes. https://www.fedramp.gov/2026/agencies/use/classes/