The Proposed FAR Controlled Unclassified Information Rule

A Plain Language Brief for Management and Executive Leadership

David W. Koran
CyberAB Registered Practitioner Advanced
June 2026

Summary

The federal government is moving to standardize how its contractors protect sensitive but unclassified government information. For years, obligations of this kind fell mainly on Department of Defense contractors through the Defense Federal Acquisition Regulation Supplement and the Cybersecurity Maturity Model Certification program. A proposed rule now folds comparable requirements into the Federal Acquisition Regulation, the rulebook that governs civilian and defense contracts alike. The rule reaches across the federal contracting base, but the operative trigger is whether a given solicitation or contract identifies Controlled Unclassified Information through a new standard form. Purchases of commercial off-the-shelf products remain outside its scope.

For companies that will handle this information, the rule does more than add a security requirement. It places cyber readiness into the offer itself, defines how subcontractors and cloud providers must be selected and managed, and assigns the government a documented role in identifying what must be protected. The sections that follow translate those points into the decisions that belong at the leadership level.

What Controlled Unclassified Information Means

Controlled Unclassified Information, commonly shortened to CUI, is government information that is sensitive but not classified. It is information the government owns, or that a company creates or holds on the government's behalf, which a law, regulation, or government-wide policy requires to be protected. It sits between two familiar categories. It is more sensitive than ordinary business information, and less sensitive than classified material, which carries its own separate and stricter rules.

For a manufacturer, CUI often takes the form of technical drawings, engineering specifications, production data tied to a government program, or export-controlled information. The common thread is that the information matters to national or economic security, and the government has decided it must be safeguarded wherever it travels, including on a contractor's own systems.

What Is Changing

Two shifts matter most for leadership. The first is reach. Until now, the requirement to protect this category of information applied chiefly to defense work. The proposed rule applies a comparable expectation to contracts across the federal government, with the narrow exception for commercial off-the-shelf purchases. A company that has never

considered itself a cybersecurity-regulated business may find these obligations attached to a civilian agency contract.

The second is clarity of identification. The rule introduces a standard form that the government includes with solicitations and contracts. The form states plainly whether the work involves CUI and, if it does, which categories apply. In the past, contractors were often left to determine on their own whether information in their possession was controlled. The form shifts much of that identification responsibility to the government, although a contractor must still speak up if it encounters sensitive information that the form did not anticipate.

What the Rule Requires

A contractor that handles CUI must protect it in accordance with a recognized federal security standard. For the contractor's own systems, the rule points to the National Institute of Standards and Technology publication SP 800-171, in its third revision, applied using the parameter values specified by the government. Two adjacent paths exist. When a contractor operates a system on the government's behalf, agency-identified controls from NIST SP 800-53 apply instead. For information tied to a designated critical program or a high-value asset, an agency may add selected enhanced requirements from NIST SP 800-172. For most manufacturers, the first path, SP 800-171, will govern daily operations.

A contractor must report a security incident involving CUI within 72 hours of discovering it. This window aligns with the long-standing defense reporting timeline and replaces a far shorter window that appeared in an earlier draft and drew significant objections from industry.

A contractor must ensure that employees who handle CUI understand and follow the applicable handling requirements. The proposed rule deliberately steps back from a single mandated training program, giving contractors flexibility in how they confirm that their people have the knowledge and skills to comply. A contractor must also make its system security plan available to the government on request. That plan is the document that describes how the company protects information and, as noted below, must account for external providers that handle it.

A contractor must also flow these requirements down to subcontractors that will handle the same information. Responsibility does not stop at the prime contractor. It extends through the supply chain. The rule recognizes that certain systems fall outside its scope, including a tightly configured virtual desktop that never stores information locally and ordinary commercial communications networks that carry traffic regardless of its source.

Readiness Becomes Part of the Bid

The most consequential change for leadership is not a single security control. It is where readiness has to exist. The solicitation provision at FAR 52.240-6 addresses the offeror directly, and it sets a low threshold with a firm obligation. If an offeror is not compliant with any requirement of the CUI clause, it must submit, as part of its offer, a disclosure identifying every requirement it does not meet, along with a plan of action and milestones to meet them. Noncompliance with even one requirement, therefore, produces a written disclosure within the proposal itself. Cyber readiness becomes part of the submission rather than a project that begins after award. A company that treats compliance as work for the implementation phase may find that it has disclosed a gap, in writing, at the moment it competed for the contract. Capture, contracts, and security need to coordinate before a proposal goes out, not after.

External Service Providers Enter the Security Plan

The rule requires that the system security plan identify any external service provider that handles CUI. For most organizations, that single requirement reaches further than it first appears. Managed service providers, hosted email, cloud file storage, backup services, governance and compliance tooling, engineering and product lifecycle platforms, and remote support vendors can all fall within it. Each becomes a documented part of the security posture that the government may ask to review. The practical task for management is to know which outside parties touch this information, to confirm that their handling meets the same standard, and to record the relationship accurately rather than discover it during a review.

Cloud Handling Carries a Specific Standard

Where a cloud service provider stores, processes, or transmits CUI identified in the contract, the rule does not leave the security bar to general judgment. It requires that the provider meet security requirements equivalent to the federal FedRAMP Moderate baseline. This turns cloud selection into a defined procurement filter. A platform widely regarded as secure is not automatically sufficient. The relevant question is whether it meets the named federal baseline or is independently assessed as equivalent to it. Organizations that already operate in compliant government cloud environments will recognize this requirement. Those relying on commercial productivity tools should examine the gap with care.

How This Relates to CMMC

For a defense contractor, much of this will feel familiar. Many defense suppliers already work toward the same security standard under existing defense rules and the Cybersecurity Maturity Model Certification program. The comparison below shows where the two regimes align and where they differ.

Topic	Defense rules and CMMC	Proposed FAR CUI rule
Who is covered	Defense contractors and their suppliers	Federal contractors when CUI is identified in the contract
Security standard	NIST SP 800-171, Revision 2	NIST SP 800-171, Revision 3
Incident reporting	Within 72 hours	Within 72 hours
How compliance is verified	Third-party certification for many contracts	Offer disclosure and documentation on request; no third-party certification
Bid stage disclosure	Assessment or certification, separate from the offer	Offer must disclose gaps, a plan of action, and milestones
Flowdown to subcontractors	Required	Required

One point in that comparison deserves a sentence of explanation. The defense certification program currently measures compliance against Revision 2 of the security standard, whereas the proposed rule references the newer Revision 3. A company that serves both defense and civilian customers could be asked to satisfy two editions of the same standard simultaneously. This is a planning matter rather than an emergency, but it belongs on the radar of anyone responsible for both lines of business.

What It Is Likely to Cost

The government published a cost analysis with the earlier version of these requirements. For a typical small business, the first-year implementation costs are estimated at around 148,000 dollars, with recurring annual costs thereafter. Two cautions apply. The estimate predates the move to the third revision of the standard, so the figure may understate the work for organizations starting from an older baseline. The actual cost depends heavily on the current security posture. A company already meeting the defense standard will spend far less than one beginning from nothing. The figures are useful as planning anchors, not as quotes.

What Management Should Do Now

A measured response begins with a few questions that do not require a consultant to answer. Determine whether your current or prospective contracts involve CUI. If you are unsure, the new standard form will eventually make the answer explicit, but you do not have to wait to begin asking.

Coordinate security readiness with your capture and contracts teams before proposals go out, as an offer may need to disclose gaps and include a plan of action and milestones. Inventory where sensitive information lives in your systems today, and which outside providers touch it, because most organizations underestimate how widely such information spreads across email, shared drives, and engineering tools.

Confirm that any cloud service handling CUI meets the FedRAMP Moderate equivalent bar. Bring your system security plan up to date so it reflects actual practice, including the external providers it must name. Finally, assign clear internal ownership. These obligations cross information technology, contracts, and operations, and they tend to fall through the gaps when no single person is accountable.

Status and Outlook

This is a proposed rule, not final law. The clause language reviewed here is part of the Revolutionary FAR Overhaul, a broad rewrite of the Federal Acquisition Regulation. The proposed rule was placed on public inspection on June 22, 2026, and is scheduled for publication in the Federal Register on June 23, 2026, as document 2026-12559, a single action running 439 pages. Publication opens a public comment period, and the text can change before any final rule takes effect. The direction, however, has held steady across administrations, because the underlying concern, protecting federal information from adversaries who target contractors as a softer entry point, does not move with political cycles. The reasonable approach is to treat this period as preparation time and to comment on where the proposed language would create practical difficulty.

Bottom Line

The proposed rule does more than add another cybersecurity requirement. It makes the handling of Controlled Unclassified Information part of contract pursuit, part of what a company discloses in its offer, part of how it selects cloud providers and manages subcontractors, and part of what executives own rather than delegate. For organizations already working toward the defense standard, it extends familiar ground, with the edition of the standard as the point to watch. For organizations new to these obligations,

this is a real shift that rewards early, deliberate preparation. The work is manageable when it begins before a contract requires it.

References

Federal Acquisition Regulation: Revolutionary Overhaul, proposed rule, document 2026-12559, scheduled for publication June 23, 2026.
https://www.federalregister.gov/d/2026-12559

Federal Acquisition Regulation: Controlled Unclassified Information, earlier proposed rule, RIN 9000-AN56.
https://www.federalregister.gov/documents/2025/01/15/2024-30437/federal-acquisition-regulation-controlled-unclassified-information

Revolutionary FAR Overhaul, FAR Part 40 materials.
https://www.acquisition.gov/far-overhaul

NIST SP 800-171, Revision 3. https://csrc.nist.gov/pubs/sp/800/171/r3/final

NIST SP 800-171, Revision 2. https://csrc.nist.gov/pubs/sp/800/171/r2/final

NIST SP 800-53, Revision 5. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST SP 800-172. https://csrc.nist.gov/pubs/sp/800/172/final

FedRAMP. https://www.fedramp.gov

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.

Cybersecurity Maturity Model Certification Program, 32 CFR Part 170.
https://www.ecfr.gov/current/title-32/part-170