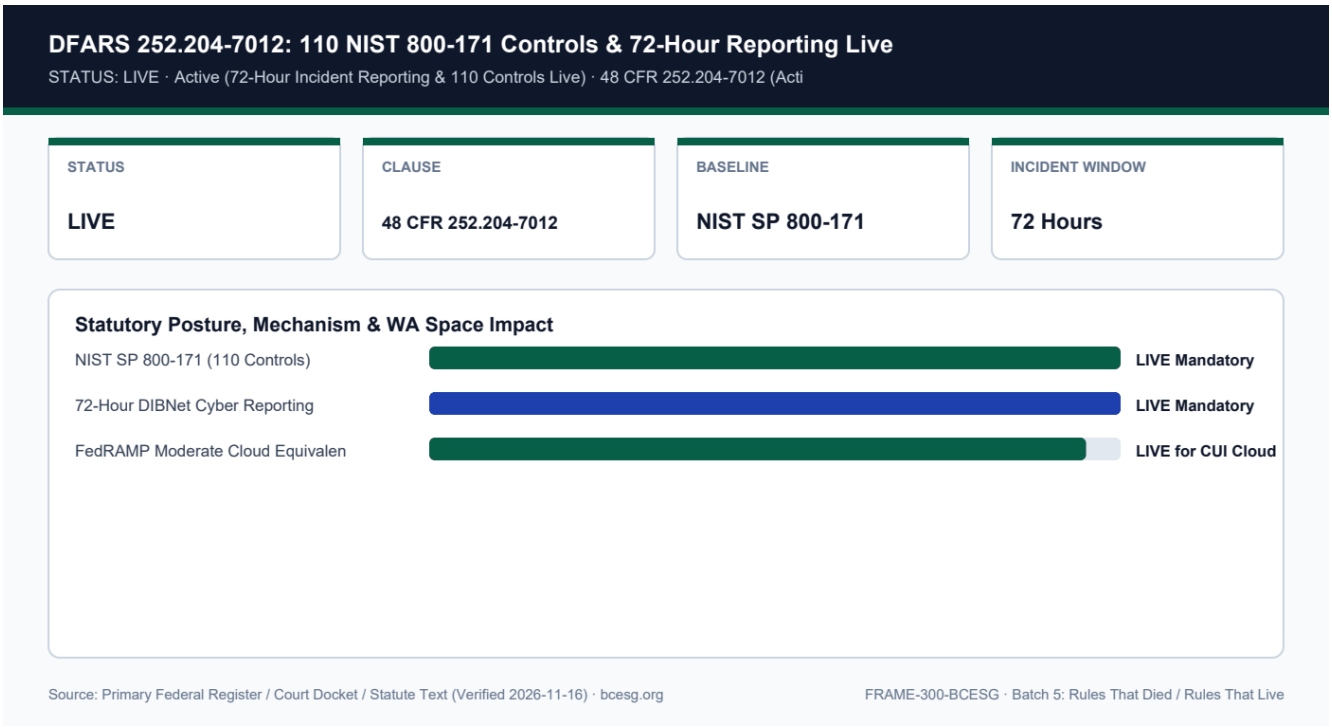
DFARS 252.204-7012 & NIST SP 800-171: LIVE — Mandatory CUI Safeguarding Regardless of CMMC Pause

Published: November 16, 2026 · Canonical URL: https://bcesg.org/wa-space-rule-dfars-7012-nist-800-171-live/

Rule: DFARS 252.204-7012 Safeguarding Covered Defense Information & Cyber Incident Reporting | **Status:** LIVE | **Instrument:** 48 CFR 252.204-7012 (Active DoD Acquisition Clause) | **Date:** Active (72-Hour Incident Reporting & 110 Controls Live)

Verdict & Proof: DFARS 252.204-7012 is LIVE and fully enforceable. DoD's July 2026 pause on CMMC Phase 2 C3PAO transitions did not suspend DFARS 7012, NIST SP 800-171 (110 controls), or 72-hour cyber incident reporting.



Obligation	Citation	Status
Adequate Security (NIST SP 800-171)	48 CFR 252.204-7012(b)	LIVE — Mandatory upon award
72-Hour Cyber Incident Reporting	48 CFR 252.204-7012(c)	LIVE — Mandatory within 72h
Cloud FedRAMP Moderate Equiv.	48 CFR 252.204-7012(b)(2)(ii)(D)	LIVE — Mandatory for external cloud

Who Owes What by When: Continuous CUI Protection

Every Washington space supplier holding a DoD prime or subcontract containing DFARS 252.204-7012 must implement NIST SP 800-171 across all systems processing Covered Defense Information (CDI/CUI), use FedRAMP Moderate-equivalent cloud services, and report cyber incidents to DoD within 72 hours.

Unlike CMMC Phase 2's paused C3PAO transition, DFARS 7012 has been continuously binding since 2017 and is actively audited via False Claims Act and DCMA DIBCAC reviews.

Batch 4 vs. Batch 5 Scope

Batch 4 detailed how primes verify DFARS 7012/SPRS scores in supplier onboarding; this Batch 5 brief establishes 7012's live legal status independent of the CMMC Phase 2 pause.

Verified Primary Sources & Internal Bridges

• eCFR 48 CFR 252.204-7012:
https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7012