Kiteworks

COMPLIANCE BRIEF

Meeting the FedRAMP Equivalency Requirement of CMMC

Protect CUI by Avoiding Empty Vendor Claims of Equivalency

What Is DFARS 7012 and Why Is It Important to CMMC Compliance?

DFARS 7012, or Defense Federal Acquisition Regulation Supplement Clause 252.204-7012, is a set of cybersecurity requirements for contractors working with the U.S. Department of Defense (DoD). It focuses on protecting controlled unclassified information (CUI) and is based on the NIST SP 800-171 standard. On the other hand, CMMC 2.0, or Cybersecurity Maturity Model Certification, is a framework that measures a company's cybersecurity maturity and readiness to work with the DoD. The relationship between DFARS 7012 and CMMC 2.0 is that they are interconnected. While DFARS 7012 focuses on specific security controls for protecting CUI, CMMC 2.0 builds on DFARS and includes maturity levels to classify the extent of an organization's cybersecurity preparedness. CMMC 2.0 encompasses all the requirements of DFARS 7012 and goes beyond by adding maturity levels and a formal third-party assessment process. Therefore, contractors need to comply with both DFARS 7012 and the specific requirements for their CMMC maturity level, with CMMC 2.0 essentially encompassing and expanding upon the DFARS 7012 framework.

For CMMC compliance, DFARS 7012, specifically paragraph (D), requires that if a contractor plans to use an external cloud service provider (CSP) to handle covered defense information (CDI), the **CSP must meet security requirements equivalent to the FedRAMP Moderate** baseline and comply with specific security measures outlined in paragraphs (c) through (g) of the clause. This means the contractor is responsible for ensuring that the CSP meets these security standards when handling CDI. CMMC 2.0 encompasses all the requirements of DFARS 7012 and goes beyond by adding maturity levels and a formal third-party assessment process. Therefore, contractors need to comply with both DFARS 7012 and the specific requirements for their CMMC maturity level, with CMMC 2.0 essentially encompassing and expanding upon the DFARS 7012 framework.

One must clearly understand what it means to be "equivalent" in order to be equivalent. Fortunately, the DoD recently released the FedRAMP Equivalency Memo, which provides guidance and clarification to what it means to be equivalent. According to the memo, to be considered FedRAMP Moderate equivalent, CSOs must achieve 100% compliance with the latest FedRAMP Moderate security control baseline via an assessment conducted by a FedRAMP-recognized Third Party Assessment Organization, provide a body of evidence to the contractor (including the System Security Plan, Security Assessment Plan, Security Assessment Report performed by the 3PAO, and Plan of Action and Milestones), and comply with DFARS 252.204-7012 requirements for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

Solution Highlights

FedRAMP Moderate Authorized

FIPS-140 compliant

Granular policy controls

3PAO security assessments

Given this clarification, there are three questions you must ask your CSP provider to ensure they comply:

1. **Have you had an assessment conducted by a FedRAMP-recognized Third Party Assessment Organization?** If they cannot do this, they are not actually considered equivalent.
2. **Can you provide a body of evidence of this assessment (including the System Security Plan, Security Assessment Plan, Security Assessment Report performed by the 3PAO, and Plan of Action and Milestones)?** If they cannot do this, they are not actually considered equivalent.
3. **Can you show me how you are compliant with DFARS 252.204-7012 requirements for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment?** If they cannot do this, they are not actually considered equivalent.

For contractors handling sensitive government data and striving to maintain compliance with stringent defense cybersecurity regulations, validating appropriate security capabilities can represent an arduous task. However, by leveraging partners who have already completed rigorous certifications like FedRAMP Moderate Authorized, organizations can efficiently verify security posture rather than attempting extensive independent control evaluations. With a long-standing history of compliance certifications like FedRAMP, FIPS, and SOC 2, Kiteworks enables contractors to quickly validate conformity with standards like DFARS 7012 and CMMC 2.0, speeding procurements and avoiding risks from noncompliant "equivalent" partners. With feature-rich capabilities secured via continuous independent testing and auditing, Kiteworks' solutions empower contractors to meet DoD requirements with confidence while strengthening data protections through leveraging a mature, battle-tested platform.