

CMMC Phase II Program Update

사이버보안 성숙도 모델 인증(CMMC, Cybersecurity Maturity Model Certification) 2단계 프로그램 업데이트

2026년 7월 13일, 미 국방부(DoW)는 CMMC 2단계로의 전환을 즉시 유예한다고 발표했습니다. 이것이 의미하는 바는 다음과 같습니다.



핵심요약 (Key takeaway)

미 국방연방조달규정보충서(DFARS) 및 자체 평가 의무는 여전히 유효하며, 60일간의 검토는 CMMC를 폐지하는 것이 아니라 개편할 것으로 예상됩니다. 현재 미 국립표준기술연구소(National Institute of Standards and Technology)의 보안기준인 NIST SP 800-171에서 규정하는 정책과 절차를 계속 유지하는 계약자는 어떤 프레임워크의 변경이 있든 수주 경쟁에서 더 유리한 위치를 점할 것입니다. 특히, DFARS 7012 조항이 적용되는 경우에는 여전히 계약상 의무로서 NIST SP 800-171를 준수해야 합니다.

무엇이 변경되었습니까?

- **DoW는 CMMC 2단계로의 전환을 유예**했습니다. 당초 2026년 11월 10일로 예정되어 있던 CMMC 2단계는, 해당되는 계약에서 제3자 평가기관(C3PAO)의 레벨 2 인증을 요구합니다.
- **CMMC 프로그램에 대한 60일간의 "전면적" 검토가 시작**되었습니다. 이는 사이버보안을 유지하면서도 방위산업에서의 부담을 줄이는 대안을 평가하기 위함입니다.
- **잠정적으로 자체평가 및 선별된 정부주도진단**을 통해 NIST SP 800-171 개정 2판을 준수하는 것으로 전환됩니다.

무엇이 그대로 유지됩니까?

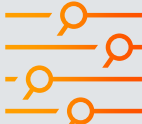
- **1단계 자체평가 요건은 그대로 유지**됩니다. CMMC 레벨 1 및 레벨 2 자체평가 규정은 이번 일시 중단에 영향을 받지 않습니다. 여기에는 레벨 2 자체평가와 관련된 "보안개선계획(POA&M)"을 완료하는 데 180일이 소요되는 것과 조건부 인증을 NIST SP 800-171 요건으로 제한하는 것이 포함됩니다.
- **NIST SP 800-171 요건은 변경되지 않았습니다.** DFARS 252.204-7012에 따른 보호대상 국방정보 보호 의무는 모든 계약자와 하도급업체에 계속 적용됩니다.
- **주 계약업체들이 준비 일정을 계속 주도하고 있습니다.** 이미 많은 주 계약업체들은 정부의 due date보다 앞서 협력업체 준비 완료일을 설정했으며, 연방 정부의 일시 중단과 상관없이 NIST SP 800-171 이행 증거 또는 변경되지 않은 CMMC 1단계 요구사항(CMMC 준비 상태)을 계속 요구할 것으로 예상됩니다.

변경되지 않은 CMMC 1단계 요건 :



3년

인증을 유지하기 위해 CMMC 자체 평가를 완료하는 주기



110개

NIST SP 800-171 개정 2판의 모든 보안 요구사항은 여전히 요구되며, "시스템 보안 구현 현황문서(SSP)"에 문서화



매년

준수확인서는 여전히 "DoD 공급업체 보안 평가 시스템 (SPRS)"에 입력



180일

진단 결과에서 나온 "보안개선계획(POA&M)" 항목들을 정리하기 위한 기간