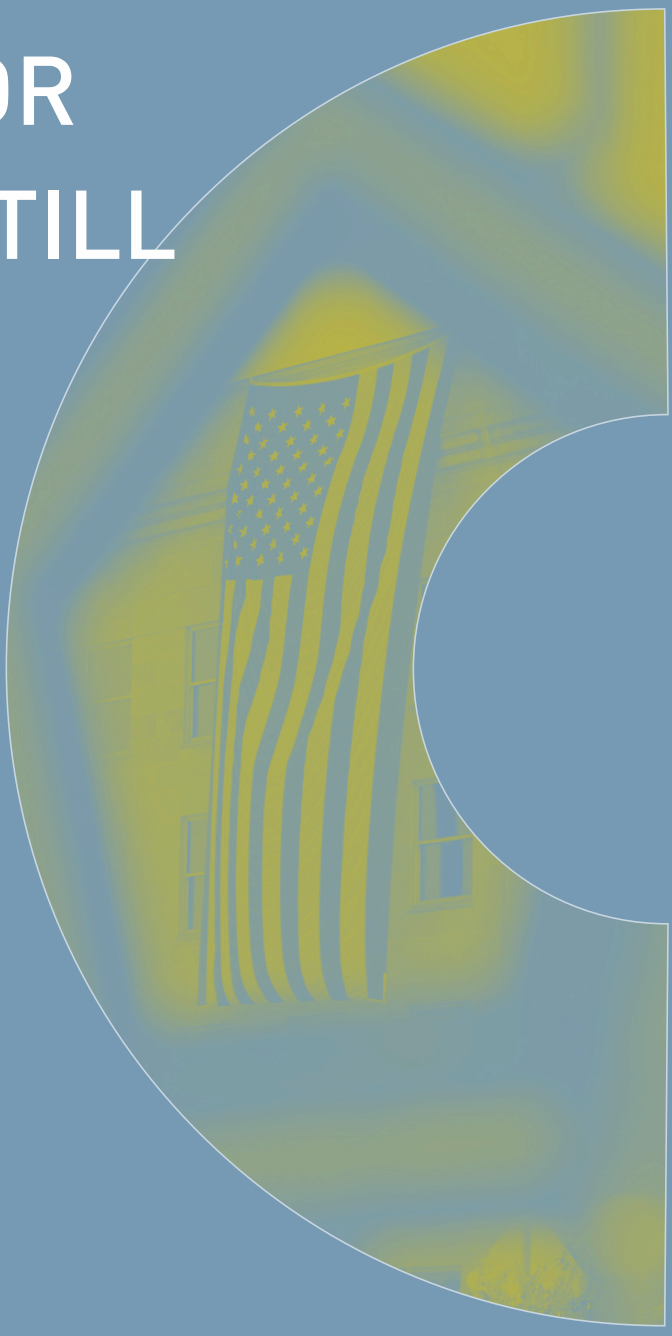
CMMC

CYBERSÄKERHETS-CERTIFIERING FÖR LEVERANTÖRER TILL USA:S FÖRSVAR



FAKTABLAD

Cybersäkerhetscertifiering för leverantörer till USA

→ Vad är CMMC?

- **Cybersecurity Maturity Model Certification (CMMC)** är ett cybersäkerhetsramverk som har utvecklats av USA:s försvarsdepartement (DoD) för att säkerställa att hela leveranskedjan tillämpar lämpliga skyddsåtgärder för Federal Contract Information (FCI) och Controlled Unclassified Information (CUI).
- CMMC grundar sig på tidigare existerande krav i NIST SP 800-171, men tillför ett nytt certifieringssystem där efterlevnaden valideras genom självutvärdering eller tredjepartsbedömning, beroende på säkerhetsnivå. I den aktuella versionen, CMMC 2.0, delas kraven in i tre säkerhetsnivåer:
  - Nivå 1 (Foundational) – 15 grundläggande åtgärder förenliga med FAR klausul 52.204-21.
  - Nivå 2 (Advanced) – 110 åtgärder i linje med NIST SP 800-171.
  - Nivå 3 (Expert) – 134 åtgärder: 110 baserade på NIST SP 800-171 och 24 på NIST SP 800-172.
- CMMC har således formaliserat ett minimikrav på cybersäkerhet och ersätter tidigare förlitande på självdeklaration (self-attestation).

→ Vem träffas av CMMC?

CMMC är obligatoriskt för alla företag som är en del av DoD:s försörjningskedja och som hanterar FCI eller CUI inom ramen för ett DoD-kontrakt.

- Kraven träffar både huvudleverantörer och i tillämpliga fall underleverantörer, oavsett nationalitet. CMMC-krav "flödas ner" via 'flow-down clauses', vilket betyder att även underleverantörer långt ned i kedjan kan omfattas av certifieringskrav.
- För svenska företag innebär det att även indirekt leverans till DoD, via exempelvis europeiska systemleverantörer, omfattas av CMMC om information skyddad enligt amerikanska regelverk behandlas.
- Kraven gäller oavsett företagsstorlek, vilket gör att även små och medelstora företag måste ha processer för att uppnå efterlevnad.

Cybersäkerhetscertifiering för leverantörer till USA

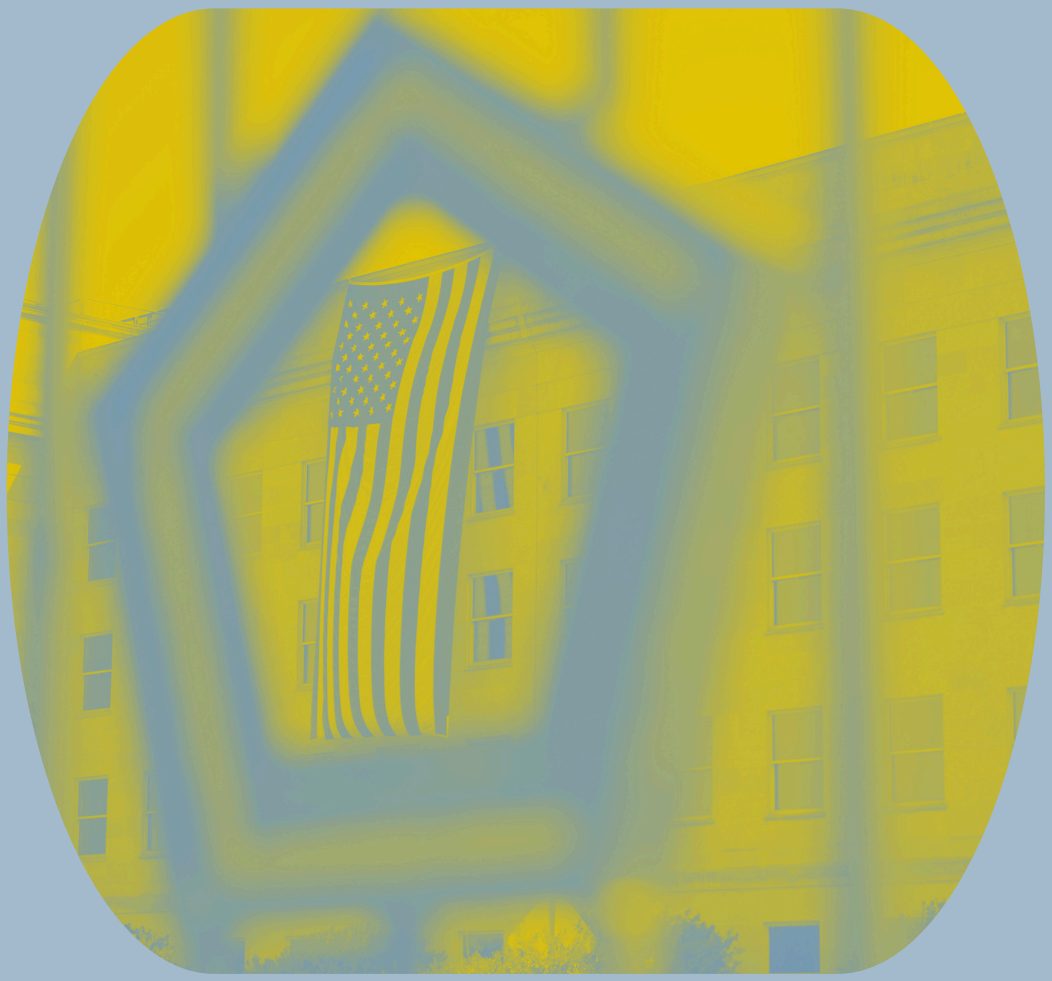
→ När blir CMMC tillämplig?

CMMC tillämpas vid upphandlingar där DoD är slutkund och där skydd av FCI eller CUI krävs enligt DFARS. CMMC 2.0 håller successivt på att implementeras i utvalda kontrakt (s.k. pathfinder contracts) och förväntas vara fullt integrerat i samtliga nya DoD-kontrakt från och med slutet av 2025.

- För nivå 1 räcker årlig självbedömning med ledningsattest.
- För nivå 2 krävs tredjepartscertifiering för "prioriterade" kontrakt, men självbedömning gäller i vissa fall.
- För nivå 3 ansvarar DoD själva för certifieringen. Tillämpningen sker alltså beroende på vilken information som behandlas och vilka villkor som framgår av kontraktets DFARS-klausuler.

→ Varför relevant för svenska företag?

CMMC är ett allt viktigare krav för att delta i försvarsrelaterade upphandlingar kopplade till DoD. Regelverket omfattar samtliga leverantörsled – från huvudleverantörer till mindre underleverantörer – och gäller oavsett geografisk hemvist. Sveriges fördjupade samarbete inom NATO medför att svenska företag i allt högre grad hanterar CUI och därmed omfattas av CMMC-krav, även indirekt genom internationella försörjningskedjor.
Avsaknad av certifiering kan utesluta företag från anbudsförfaranden, leda till kontraktsförlust, ekonomiska sanktioner och i vissa fall rättsliga påföljder enligt amerikansk lagstiftning. Dessutom ökar risken för cyberangrepp vid bristande säkerhetskontroller.
Certifiering är emellertid inte enbart ett krav, utan ett strategiskt verktyg för marknadstillträde, samarbetsmöjligheter och långsiktig affärsutveckling. En förhastad implementering inför ett specifikt kontrakt kan medföra höga kostnader och resursbelastning, medan tidig förberedelse stärker både cybersäkerhet och konkurrenskraft – även i framtida svenska upphandlingar där CMMC förväntas integreras.



SOFF

www.soff.se