

A scalable enclave for defense business growth



CyberSheath helped SEP achieve CMMC Level 2 certification with a customized enclave designed to support both current defense operations and future business development.



Client

SEP is one of Indiana's largest software development companies, with 180 employees and a client base spanning emerging scale-ups to Fortune 100 companies. Founded in 1988 and headquartered in Westfield, Indiana, SEP builds software across aerospace, life sciences, agriculture, and manufacturing, with cross-functional teams specializing in AI enablement, product design, and UX across web, mobile, desktop, embedded systems, and cloud.

Situation

The Pentagon suspended CMMC Phase 2 mandatory third-party assessments in July 2026, but the underlying cybersecurity obligations — DFARS 252.204-7012, NIST SP 800-171, and government-led DIBCAC assessments — remain in force. SEP's leadership pursued certification before the suspension, recognizing that independently verified compliance would distinguish the company from competitors regardless of the program's timeline. With many contractors now using the pause as a reason to delay, SEP's early investment in certification has become an even stronger differentiator.

The company began with an internal enterprise-wide gap assessment revealing the need for an enclave. SEP sought the assurance of outside expertise to interpret the requirements and execute the implementation on an aggressive timeline. A team conducted a structured evaluation, interviewing potential partners against a defined set of selection criteria.

CyberSheath stood out for its experience in the defense industrial base and its experience preparing clients for assessments with A-LIGN, the CMMC Third-Party Assessment Organization (C3PAO) SEP had selected to conduct its assessment. That familiarity gave SEP's leadership confidence that CyberSheath understood what A-LIGN's assessors would expect and could prepare accordingly.



Process

Adhering to NIST framework, CyberSheath designed and implemented the compliance program for SEP's secure enclave, defining the security controls, access policies, and system configurations needed to meet CMMC standards. The enclave was scoped specifically to SEP's defense operations, ensuring the company's commercial work across pharmaceuticals, agriculture, manufacturing, and engineering could continue without disruption. SEP's technical team supported key elements of the implementation, and both organizations operated under a shared responsibility model that reflected each party's ownership of specific tools, systems, and infrastructure.

Solution

The engagement was a shared effort, with SEP's technical team taking on significant portions of the implementation rather than relying solely on CyberSheath to manage the environment. CyberSheath adapted its processes to accommodate SEP's operational preferences and technical capabilities, working through the details of a shared responsibility matrix that defined which party owned which controls.

The enclave provided a secure environment for CUI handling while preserving SEP's existing workflows and operations.

Results

To validate SEP's readiness to support defense programs handling CUI, A-LIGN conducted an independent assessment of SEP's environment and practices. SEP earned a perfect 110 score on its assessment and successfully achieved CMMC Level 2 certification. Earning certification with A-LIGN confirms that SEP's software development work involving CUI is performed in a CMMC compliant environment, giving defense clients greater confidence in SEP's security posture. Just as importantly, it sets SEP up to pursue new and expanding defense work as CMMC requirements continue to roll out across Department of Defense contracts.

Insights

SEP's approach to CMMC certification followed a disciplined framework that defense contractors of any size can apply:

- » **Build the business case before the technical case.** SEP's leadership started by identifying the expected outcomes of certification — not just continued eligibility for defense work, but market distinction and new business development opportunities. That clarity on benefits informed every subsequent decision, from scoping to partner selection.
- » **Understand your total investment, not just the upfront cost.** Assessment fees and implementation costs are only part of the picture. CMMC certification operates on a three-year cycle, and the ongoing cost of maintaining compliance should factor into the business case from the beginning.
- » **Assess the maturity of your security profile early.** A realistic understanding of your current security posture leads to a meaningful gap analysis, which in turn provides reliable cost projections and a defensible implementation timeline. Starting from assumptions rather than evidence creates risk on both fronts.
- » **Select a partner and C3PAO based on your own operational needs.** SEP's team invested time in understanding how it operates before evaluating partners, which allowed it to assess fit against defined criteria rather than relying on reputation or sales conversations alone.

CyberSheath is a longtime leader in the DOD/DOW cybersecurity space and an expert in DFARS, NIST and CMMC regulations. CyberSheath solves the whole problem with a flexible approach that meets each customer exactly where they are and guides them to full compliance at the lowest possible cost.