

Streamlined Compliance for SMB Defense Contractors

CyberSheath's Federal Enclave solution helped Cutting Edge Communications achieve CMMC Level 2 certification with a targeted approach that matched their limited CUI handling requirements.



Client

Cutting Edge Communications is an engineering consulting company headquartered in Huntington Beach, California. The company provides expert personnel to support aerospace and defense contractors, with a team of more than 100 professionals serving over 20 companies ranging from large prime contractors to new startups. Cutting Edge specializes in adapting to each client's workplace and mission, offering business support from preaward proposal development through program implementation. It has built a reputation as one of the most highly regarded suppliers of qualified experts in the defense industry.

Situation

When CMMC compliance requirements took effect for defense contractors, Cutting Edge Communications faced the challenge of securing Controlled Unclassified Information (CUI) while maintaining operational flexibility. Engineers frequently work in client environments, and the organization handles minimal CUI, mostly consisting of archived materials.

Initially, company leadership believed CMMC compliance could be achieved in-house utilizing a vendor offering a compliance tool. However, early attempts with the compliance vendor revealed significant challenges. The enterprise-level policies and tools offered by the initial vendor created a mismatch with Cutting Edge's actual needs, which centered around securing a small amount of CUI rather than overhauling entire enterprise systems.

The company needed a solution that could provide both cybersecurity implementation and compliance guidance in a single, cohesive package rather than fragmented services that would require coordination across multiple vendors.

Process

Cutting Edge Communications evaluated multiple CMMC solution providers, focusing on end-to-end service, clarity in offerings and compliance support beyond just IT security implementation. The evaluation process emphasized finding a provider that could offer flexibility in pacing and a straightforward approach to certification.

CyberSheath stood out through its comprehensive methodology that addressed both technical security requirements and compliance processes simultaneously. This dual approach meant implementation streams could overlap, accelerating progress toward certification rather than handling security and compliance as separate, sequential phases.

The collaborative process included a detailed assessment of Cutting Edge's use cases, particularly understanding how CUI flowed through operations where engineers work in various client environments. CyberSheath's expertise filled gaps in the internal team's IT security knowledge while providing hands-on support throughout implementation.



Solution

CyberSheath implemented a Federal Enclave solution that precisely matched Cutting Edge's operational requirements. The enclave approach proved ideal for an organization handling minimal CUI, providing a secure workspace for sensitive information without requiring enterprisewide security overhauls.

The integrated approach to security and compliance eliminated the coordination challenges that had complicated the company's initial vendor experience. The responsive, hands-on support provided expertise where the internal team needed guidance while maintaining flexibility to adjust pacing as project demands required.

Results

Cutting Edge Communications achieved CMMC Level 2 certification through an assessment conducted by RSI Security. The assessment process proceeded smoothly without unexpected challenges, demonstrating thorough preparation and effective collaboration between CyberSheath and the Cutting Edge team.

The enclave solution provided a streamlined approach, enabling the company to maintain full operational continuity while meeting all CMMC requirements, ensuring continued ability to support defense contractor clients.



Insights

The Cutting Edge Communications team relayed these valuable lessons for small- and medium-sized businesses facing CMMC compliance:

- » **Do not attempt CMMC compliance alone** unless you have a robust IT department. The technical and compliance requirements are too complex for many businesses to handle without specialized expertise.
- » **Invest in a turnkey end-to-end solution.** For defense contractors that struggle with operating strong, mature IT and security capabilities, comprehensive providers save time, reduce risk and ensure audit readiness while avoiding wasted effort and money on partial solutions.
- » **Expect CMMC to be a full-time effort** for at least one dedicated resource. The compliance process requires significant time investment and focused attention throughout implementation.
- » **Choose providers offering flexibility and responsive support.** The ability to adjust pacing and receive hands-on guidance throughout the process is critical for successful certification.
- » **Consider enclave solutions for minimal CUI environments.** Companies handling limited Controlled Unclassified Information can often meet requirements more cost-effectively through targeted enclave approaches rather than enterprisewide implementations.

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.