CASE STUDY

Ready for Business

CyberSheath Helps CIS Secure Achieve CMMC Level 2 Certification Ahead of Schedule

Client

CIS Secure is an end-to-end provider of the broadest portfolio of powerful communications and cybersecurity solutions designed, integrated and supported by subject matter experts of the Department of Defense/War (DOD/DOW) and intelligence communities. The company is an ISO 9001 and NSA Certified TEMPEST manufacturer and test facility for secure collaboration, tactical communications and protected personal mobility solutions. Headquartered in Ashburn, Virginia, CIS Secure pushes the boundaries of design and innovation to create compelling and secure collaboration solutions.

Situation

When the DOD/DOW announced that members of the Defense Industrial Base (DIB) would need to achieve Cybersecurity Maturity Model Certification (CMMC) compliance to continue doing business, CIS Secure took immediate action. With CMMC 2.0 requirements taking effect starting Nov. 10, 2025, achieving CMMC Level 2 was crucial for maintaining the company's ability to serve customers and protect sensitive information it was entrusted with.

One of the major challenges was aligning business units with disparate security maturity under a unified approach to meet CMMC requirements. This involved restructuring parts of the network and expanding the scope from isolated enclaves to an enterprise-wide strategy.

CIS Secure's gap analysis revealed several key challenges, including policy misalignment across divisions and a misunderstanding of which business units were in scope for CMMC. The company needed expert guidance to address these complex technical and organizational requirements efficiently.

Process

CIS Secure partnered with CyberSheath to assist with technical implementation and alignment. CyberSheath's collaborative approach provided the expertise needed to address complex technical and organizational requirements efficiently.

CyberSheath operates as an extension of its clients, performing IT, compliance and security functions to help them achieve and maintain their goals. The process with CIS Secure included:

- **Comprehensive gap analysis** — Identifying policy misalignments across divisions and clarifying which business units were in scope for CMMC requirements.
- **Technical implementation and system configuration** — CyberSheath's expertise significantly reduced the effort required to configure systems and controls to meet CMMC requirements.
- **Living documentation approach** — Treating the SSP and POAM as living documents, updating them throughout the process to track progress and assign responsibilities.
- **Prioritized remediation** — Addressing gaps based on time and resources needed, starting with those requiring new equipment.

- **Policy and procedure overhaul** — Extending the scope to include end-user devices rather than just enclaves and covering all business units under unified policies.
- **Training implementation** — Using CISA and KnowBe4 programs delivered through the internal learning platform.
- **Documentation alignment** — Organizing evidence collection methodically and aligning documentation directly to the CMMC assessment matrix for easy assessment-day access.

Solution

The collaborative partnership leveraged both CIS Secure's internal cybersecurity team and CyberSheath's expertise, providing a deep bench of knowledge and experience.

Prior to the formal assessment with Cybersec Investments, a C3PAO, CIS Secure conducted a thorough internal audit of all documentation and evidence. CyberSheath was instrumental in swiftly resolving any last-minute issues, ensuring no surprises on assessment day.

Results

The assessment proceeded smoothly without any unexpected challenges. The thorough preparation and CyberSheath partnership ensured seamless assessment execution.

The team meticulously reviewed the SSP and evidence in the weeks leading up to the assessment, meeting multiple times per week to check and cross-check each other's work.

CyberSheath team members supported the assessment process and helped resolve any technical questions.

At the assessment's completion, Cybersec Investments certified that CIS Secure achieved perfect CMMC Level 2 compliance with a score of 110 — fully aligned with the 110 NIST 800-171 controls that form the basis for CMMC 2.0 Level 2 classification.

Insights

The CIS Secure team offered several lessons to other defense industry businesses:

- **Start early.** The process takes longer than expected. CMMC requirements are now phasing into contracts starting Nov. 10, 2025, and the compliance process requires significant time investment.
- **Ensure leadership buy-in.** This is critical for resource allocation and prioritization throughout the certification process.
- **Engage trusted partners.** Partnering with experienced cybersecurity experts and proven C3PAOs can greatly reduce risk and provide essential expertise for technical implementation and assessment preparation.
- **Plan for organizational changes.** Acquisitions, restructuring or rescoping can impact your compliance path and timeline.
- **CMMC compliance requires ongoing management.** Achieving certification is only the beginning — maintaining compliance requires regular documentation reviews, continuous monitoring and proactive updates to controls as threats and requirements change.

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.*

855.384.8070 | sales@cybersheath.com | cybersheath.com

CYBERSHEATH