CASE STUDY

CYBERSHEATH

Kampi Components Co., Inc.
Serving Government and O.E.M.

Managing multiple service providers for seamless CMMC compliance

CyberSheath helped Kampi Components achieve CMMC Level 2 certification by addressing noncompliant service providers and coordinating a complex multivendor environment.

Client

Kampi Components Co., Inc., is a military parts distributor based in Fairless Hills, Pennsylvania. Founded in 1984, Kampi provides distribution and logistical support for government and defense contractors, including procurement, inspection, testing, packaging and transportation of military equipment and replacement parts. The company employs about 65 people and operates from a 36,000-square-foot facility, serving a long-standing role within the Defense Logistics Agency and broader Department of Defense/War (DOD/DOW) supply chain.

Situation

When the DOD/DOW conducted an unexpected DIBCAC High Assessment at Kampi's facility, the company faced immediate pressure to achieve full CMMC Level 2 compliance. The audit revealed gaps that needed addressing before Kampi could pursue formal certification.

The company had not yet completed its planned migration from a commercial cloud infrastructure to Microsoft's Government Community Cloud (GCC High). Kampi also relied on multiple managed service providers (MSPs) for various IT functions, including a major MSP handling help desk support and network operations center services. None of these external service providers were CMMC compliant, and some had no plans to pursue certification or support the compliance requirements. Under CMMC requirements, noncompliant service providers with access to Controlled Unclassified Information (CUI) environments become compliance obstacles that can prevent successful certification.

As a distribution company with warehouse operations handling military materials, Kampi also needed comprehensive physical security controls, including visitor management, access control systems, secure storage for CUI in both digital and physical formats, and monitoring capabilities across its entire facility.

Process

Following the government audit, Kampi engaged CyberSheath to develop a comprehensive compliance strategy. CyberSheath's initial gap assessment aligned closely with the government's findings, confirming the scope of work and establishing a clear road map to certification.

The collaborative process included:

- **Cloud infrastructure migration:** Moving Kampi's entire environment from commercial cloud services to GCC High while maintaining operational continuity.
- **Service provider remediation:** Evaluating all external service providers' compliance status and determining remediation paths.
- **Physical security implementation:** Establishing comprehensive controls across Kampi's facility, including infrastructure security, visitor management systems, badge readers, surveillance cameras, alarm systems and secure storage for physical CUI materials.

- **Documentation preparation:** Developing a System Security Plan (SSP) and Plan of Action and Milestones (POAM) aligned to CMMC assessment requirements.

Solution

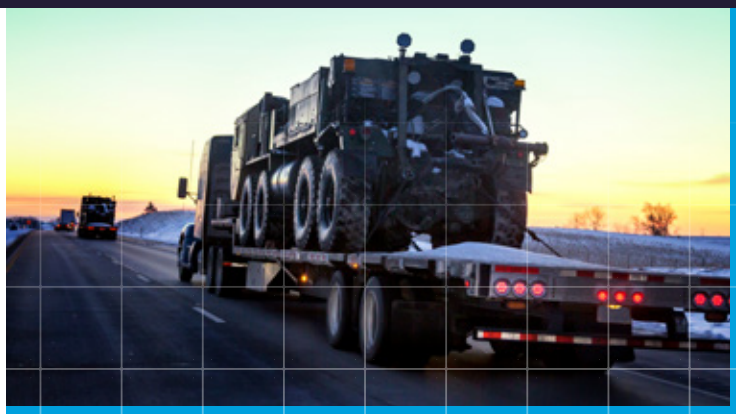
CyberSheath implemented a GCC High managed services solution that provided the FedRAMP-authorized platform Kampi needed for handling CUI. The solution created a fully compliant technology environment by eliminating noncompliant service providers and implementing controls across both digital and physical operations.

For Kampi's warehouse and office operations, CyberSheath worked with the company to plan and implement security controls for the entire 36,000-square-foot facility with monitoring, access controls and procedures for handling CUI materials in all formats.

Results

Kampi achieved CMMC Level 2 certification with a perfect score of 110 out of 110 points with the certification assessment conducted by Cybersec Investments. The certification proceeded smoothly without unexpected challenges.

Despite the complexity of removing service providers from the environment with less than 30 days to assessment, rapid execution ensured Kampi met its certification timeline. The company maintained full operational continuity throughout the compliance process with no disruption to its distribution services.



Insights

The Kampi engagement highlights several critical considerations for defense contractors pursuing CMMC certification:

- **Evaluate all external service providers early.** Any MSP or vendor with access to CUI must be assessed within your CMMC scope based on its role and level of access. Cloud providers must hold FedRAMP Moderate (or equivalent) authorization if processing CUI.
- **Government audits can happen before formal certification.** DIBCAC assessments may occur at any time, providing an early indication of compliance gaps. Having an accurate understanding of your security posture before government audits helps avoid False Claims Act exposure.
- **Physical security and digital security require equal attention.** Organizations with on-premise operations, warehouses or facilities where CUI exists in any form must implement comprehensive physical controls beyond cloud-based security.
- **Rapid remediation is possible with experienced partners.** Even significant changes like removing embedded service providers can be accomplished quickly when working with compliance partners who understand both technical requirements and assessment processes.

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