

A Perfect 110

With CyberSheath support, Chenega Corporation achieved a perfect score in the Joint Surveillance Voluntary Assessment (JSVA) for CMMC compliance.



Client

Chenega is a highly successful Alaska Native village corporation, a group of SBA 8(a) small businesses and larger businesses offering a wide range of services — from military, intelligence and operations support to professional services and more — to the U.S. Department of Defense (DOD), government entities and corporate customers. Headquartered in Alaska, the company also operates out of multiple offices in Virginia and Texas.

Situation

Chenega was well aware of CMMC's new, stricter requirements for managing Controlled Unclassified Information (CUI) that took effect in December 2024. The management team decided outsourcing was a more efficient, expeditious approach than adding staff to comply.

Chenega executives met with a number of large, well-known service providers in the CMMC space and found their fees to be prohibitively expensive, with some doubt as to whether they had the experience and in-house capability breadth required to ensure full compliance.

Company leadership ultimately chose CyberSheath for its extensive experience, ability to deliver 100% ongoing compliance and plain-speaking approach. They also engaged a CMMC Third-Party Assessment Organization, or C3PAO, to conduct the CMMC-mandated independent compliance certification.

Process

At CyberSheath, we meet our clients where they are. Where Chenega was: a high self-assessment score but short of full compliance, which made remediation and documentation the focus of CyberSheath's AIM™ (Assess, Implement, Manage) process:

- Confirm and document the internal assessment.
- Develop and file the required System Security Plan (SSP) and a Plan of Action and Milestones (POA&M) in the U.S. Supplier Performance Risk System (SPRS) database.
- Identify and execute remediation/implementation projects that included CyberSheath personnel selecting, deploying, configuring and supporting the required technology — accurate scoping of CUI across the organization and installation and custom configuration of the Microsoft Azure architecture, including setting up secure servers, help desk and change management framework.
- Final testing and documentation — create maximum assurance that Chenega was ready for the C3PAO assessment and certification process.
- Support engagement with the C3PAO.



Solution

Due to Chenega's complex business structure — four strategic business units and more than 50 companies — CyberSheath's Federal Enclave product was the optimal solution because it did not require extensive changes to individual Chenega companies' IT and other systems.

An enclave is a highly secure, centralized "lockbox" for housing CUI outside of a client's IT systems that is fast and cost-effective to implement. Our Federal Enclave solution is managed and monitored 24/7/365 by U.S.-based CyberSheath personnel and accessible only by vetted, credentialed Chenega personnel and subcontractors. The Federal Enclave includes all of the people, processes and technologies required for full compliance, all at one firm, fixed monthly price.

Federal Enclave is a good example of the management component of CyberSheath's AIM approach: We get our clients 100% compliant, and then we manage the solution to ensure that they remain compliant on an ongoing basis.

Results

Chenega selected C3PAO Cybersec Investments for its clear, practical approach to independent third-party assessment and certification. CyberSheath led preparation and organization of materials for the review process.

- Key CyberSheath project team members were on hand to support Chenega subject matter experts, help answer questions and present documentation.
- Cybersec's lead assessor remarked upon the complete and well-organized documentation, which he said significantly expedited the assessment.
- The objective: to ensure to the C3PAO's satisfaction that all CUI data is properly secured and protected in accordance with all CMMC requirements.

At the conclusion of the assessment process, Cybersec certified that Chenega was 100% CMMC compliant, with a perfect score of 110 — fully aligned with the 110 NIST 800-171 controls that form the basis for the CMMC 2.0 Level 2 classification.

Insights

The Chenega engagement offers a few lessons to other defense industry businesses:

- » **Start now.** CMMC is now in force, and its mandates are starting to appear in DOD RFP and RFQ documents. The compliance process takes time. Don't put DOD business in jeopardy because you're noncompliant when an opportunity arises.
- » **Queues are forming for C3PAO reviews.** There is a limited number of C3PAOs, and demand is increasing. Growing C3PAO backlogs could delay certification. Begin talking to C3PAOs now, and look for one whose approach best fits your situation. Based on the assessor, that approach can vary from rigid to more flexible and practical.
- » **CMMC compliance is not an end state.** CMMC compliance is a continuous effort. Once the systems are in place, they must be monitored and managed. An experienced managed service provider (MSP) assures — and documents — full, ongoing compliance.
- » **Know what you're buying.** Don't overspend and undercomply. Be clear on roles, the services your company is buying and deliverables. Clarity is key. Seek an experienced MSP who explains in clear, simple terms what is required, what they will do to deliver it and what it will cost.

CyberSheath is a longtime leader in the DOD 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.