CASE STUDY

How Tunnell Consulting Cut CMMC Costs Without Cutting Corners

CyberSheath helped Tunnell Government Services achieve CMMC Level 2 certification with a cost-effective enclave approach tailored to the Company's personnel-focused operations.

Client

Tunnell Consulting Inc. employee-owned professional services firm founded in 1962 and headquartered in Berwyn, Pennsylvania offering specialized scientific and technical expertise to government agencies and commercial clients.

Tunnell Government Services, a wholly owned subsidiary of Tunnell Consulting, Inc., provides scientific and technical consulting to federal agencies, including the Department of Defense/War (DOD/DOW), the Department of Health and Human Services, and the Department of Homeland Security. The Company sources and places specialized SMEs (subject matter experts) to support government missions in areas such as public health preparedness, biomedical research, and laboratory operations.

Situation

Tunnell Government Service's primary business model centers on identifying, vetting, and placing qualified consultants into government positions. These consultants typically work on-site at government facilities or remotely using government furnished equipment, meaning Tunnell's own systems handle CUI on a limited basis.

The Company initially pursued enterprise-wide Cybersecurity Maturation Model Certification compliance, which would have required migrating all users and systems to meet cybersecurity requirements. That approach would have imposed unnecessary licensing costs and operational burden on the broader organization, given that only a small fraction of its workforce needed access to CUI-related systems.

Process

CyberSheath worked with Tunnell's leadership team to shift from an enterprise model to a targeted enclave strategy. The collaborative process included:

- **Scope assessment and cost optimization** – Determining that only 20 of Tunnell's 242 resources required access to the compliant environment, dramatically reducing licensing and infrastructure costs compared to the original enterprise approach.

- **Enclave design** — Building an Azure Virtual Desktop (AVD) environment in Microsoft's Government Community Cloud (GCC), providing a secure workspace for CUI without changes to the company's existing commercial systems.
- **Forward-looking data protection** — Developing a secure staging area using a FedRAMP-authorized file-sharing platform to handle personnel screening and vetting information. While the government does not currently classify this data as CUI, Tunnell's leadership recognized it could be designated as such in the future. CyberSheath configured the platform per the provider's customer responsibility matrix and integrated its logs for monitoring.
- **Documentation development** — Preparing all compliance materials through CyberSheath's AIM (Assess, Implement, Manage) methodology, with Tunnell's leadership actively reviewing and refining documents to ensure accuracy.

Solution

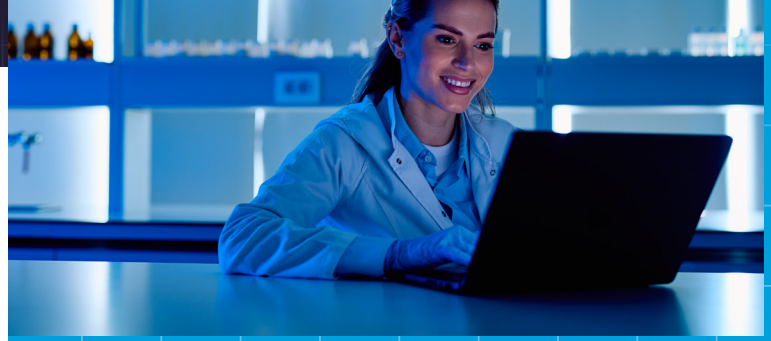
CyberSheath delivered an AVD enclave hosted in GCC, limiting the compliance scope to the 20 users who needed CUI access. Employees outside that group continued working in Tunnell's commercial environment with no disruption or additional licensing costs.

The secure staging area addressed a challenge specific to personnel-focused contractors: collecting sensitive screening documents from prospective hires — who may submit from personal email accounts or outside domains — without introducing that data directly into the enclave. The staging area served as a controlled intake point for documents, where they were received, vetted, and moved into the CUI environment as needed.

Results

Tunnell Consulting achieved CMMC Level 2 certification with a perfect score of 110 through an assessment conducted by Cybersec Investments. The assessment was completed ahead of schedule, with no pushback from auditors on documentation or evidence.

Tunnell's leadership played a direct role in that outcome, reviewing compliance documentation, challenging narratives for accuracy, and adding operational context that strengthened the materials for assessment. The enclave approach kept costs proportional to Tunnell's actual CUI footprint, avoiding the significantly higher expense of enterprise-wide GCC licensing.



Insights

Right-sizing compliance reduces cost without sacrificing security.

For organizations where CUI handling is concentrated among a small number of users, an enclave strategy can deliver the same security outcomes at a fraction of the enterprise-wide cost.

Personnel-focused contractors face unique challenges.

Companies that place consultants into government roles handle sensitive vetting data that may not currently be classified as CUI but could be in the future. Planning for that possibility now avoids costly retrofitting later.

A secure staging area can extend protection without expanding the enclave.

Integrating a FedRAMP-authorized platform — with proper configuration and log monitoring — provides a controlled intake point for sensitive data without broadening the compliance boundary.

Active client participation accelerates assessments.

When leadership engages directly with compliance documentation, it produces more accurate materials and smoother audit outcomes.

__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