CYBERSHEATH

CTG FEDERAL

CASE STUDY

CTG Federal Achieves CMMC Level 2 Certification

CTG Federal has achieved Cybersecurity Maturity Model Certification (CMMC) Level 2 following an independent assessment conducted by Cybersec Investments, a Certified Third-Party Assessor Organization (C3PAO). CyberSheath provided implementation support and advisory services during preparation and validation activities leading up to the assessment.

Organization

CTG Federal, a Cohesive Technology Group company, is a U.S. based small business delivering advanced information technology infrastructure and services to federal defense, intelligence, and civilian agencies. Headquartered in Reston, Virginia, the company designs, integrates, and supports mission-ready platforms including high-performance computing environments, sovereign AI architecture, enterprise data infrastructure, secure networking, hybrid cloud platforms, and cybersecurity solutions.

CTG Federal regularly supports programs operating in sensitive mission environments where secure handling of Controlled Unclassified Information (CUI) is required.

Requirement

As the Department of War implements the Cybersecurity Maturity Model Certification framework across the defense industrial base, contractors that store, process, or transmit CUI must demonstrate compliance with the security controls defined in CMMC Level 2, aligned with the NIST SP 800-171 standard.

To maintain eligibility for defense programs requiring validated cybersecurity maturity, CTG Federal implemented the controls, processes, and operational practices required to meet the CMMC Level 2 standard.

Implementation

CTG Federal conducted a comprehensive internal assessment against the NIST SP 800-171 control framework to evaluate existing capabilities and identify areas requiring additional implementation or documentation.

A central focus of the effort was accurately defining the compliance boundary for systems and personnel responsible for handling CUI. By mapping where CUI resides and how it moves through the organization, CTG Federal implemented a secure environment designed specifically to support those activities.

CyberSheath provided supporting services during the implementation phase, assisting CTG Federal's internal team with control alignment, documentation preparation, and readiness activities in advance of the independent assessment.

Security Architecture

The resulting environment was designed to support secure handling of CUI while maintaining a clearly defined and manageable compliance scope. The architecture incorporates:

- Access-controlled systems and networks supporting CUI processing
- Role-based access restrictions for authorized personnel
- Technical safeguards aligned with NIST SP 800-171 requirements
- Documented operational procedures governing handling and protection of CUI
- Continuous monitoring and security management practices

This approach allows CTG Federal to maintain strong protection for controlled information while limiting compliance requirements to systems and personnel directly involved in CUI handling.

Assessment

Following completion of implementation and internal readiness activities, CTG Federal underwent an independent CMMC assessment conducted by Cybersec Investments. The assessment validated that CTG Federal's systems, processes, and operational practices satisfy the requirements for CMMC Level 2 certification.

Outcome

With certification complete, CTG Federal is positioned to continue supporting the Department of War and other U.S. Federal programs requiring validated protection of Controlled Unclassified Information as CMMC requirements are incorporated into defense contracts across the industrial base.

The certification reflects CTG Federal's continued investment in cybersecurity, disciplined operational practices, and responsible stewardship of government information entrusted to its care.

Considerations for Defense Contractors

CTG Federal's certification effort highlights several practical considerations for organizations preparing for CMMC implementation:

Defined compliance boundaries reduce complexity

Organizations that clearly identify where CUI resides can limit the number of systems and users subject to CMMC controls, reducing implementation complexity and long-term compliance overhead.

Operational maturity is as important as technical controls

Successful certification requires repeatable processes, trained personnel, and documented procedures in addition to the technical safeguards required by NIST SP 800-171.

Early preparation improves assessment outcomes

Organizations that conduct internal readiness reviews and align documentation prior to the independent assessment are better positioned for an efficient and successful certification process.

__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