CMMC Level 2, Done Right: How Hire A Cyber Pro Guided a Government Contractor to 110/110—On Time, On Budget

Author: Hire A Cyber Pro, LLC

Contact: contact@hireacyberpro.com | www.hireacyberpro.com

Date: October 24, 2025

Executive Summary

A mid-sized DoD subcontractor with ~650 employees and only two full-time IT personnel needed to achieve CMMC Level 2. Core IT was co-managed by an MSP, and only two departments required access to FCI and CUI. Hire A Cyber Pro led from a free consultation through a successful C3PAO assessment. We began with CUI scoping and planning, selected a commercial off-the-shelf (COTS) secure enclave to maximize inherited controls, and executed an eight-month program: six months implementing 30+ controls per month, month 7 for System Security Plan (SSP) development, and month 8 for evidence collection and assessment preparation. Hire A Cyber Pro can move faster, but this client chose a steady cadence that aligned with a comfortable monthly budget. Because the customer was already handling CUI and acted early, the project proceeded without deadline pressure or lost-opportunity risk. The organization passed with 110/110.

Client Snapshot

- Industry: Defense subcontractor (manufacturing/engineering)
- Size: ~650 employees; 2 internal IT staff
- IT model: Co-managed with an MSP
- Regulatory scope: CMMC Level 2 (NIST SP 800-171), two departments handling FCI/CUI
- Goal: Achieve certification quickly and sustainably without building GCC-High or an on-prem enclave

The Challenge

- Lean staffing: two internal IT professionals.
- Selective scope: only two departments need CUI access.
- Time-to-value: preserve bid eligibility and subcontractor relationships.
- Audit-readiness: clean, complete, easily validated evidence for the C3PAO.

Our Approach

1) Complimentary Consultation

We start with a free discovery call to align objectives, timelines, and constraints to a workable plan.

2) CUI Scoping & Planning (Weeks 1–4)

- Business workflows: diagram how work is performed and where FCI/CUI appears.
- CUI data mapping: how CUI enters, is used, and exits; paper vs. digital; email, portals, removable media, printing, archival.
- People & roles: identify exactly who touches CUI and enforce least privilege.

- Systems & special assets: inventory devices, apps, lab systems, service accounts that process/transmit/store CUI.
- Boundary definition: minimize scope to essential users and systems.

3) Solution Selection (Weeks 3–6)

Options considered: enterprise GCC-High, on-premises stand-alone/air-gapped enclave, and a COTS secure enclave. We selected a COTS enclave given the small user base, accelerated inherited controls from a FedRAMP-authorized provider, and the customer's preference to avoid heavy migration/build efforts.

4) High-Level Gap Assessment (Weeks 5–7)

Mapped the enclave's inherited controls to the 110 NIST SP 800-171 requirements and identified residual customer obligations—policies, training, identity hygiene, media handling, physical protections, IR, VA/patching, and change control—producing a right-sized remediation plan.

5) Build, Document, and Operationalize (Months 1–6 — 30+ controls/month)

- Policy & governance: ISP; Alternate Work Site; AC, IA, CM, IR, MP, PE, RA, SI policies.
- Risk & readiness: enterprise risk assessment; tabletop exercise; corrective-action tracking.
- User enablement: user acknowledgement forms covering responsibilities, removable media, and data handling.
- Secure enclave configuration: MFA, admin separation, logging, VA cadence, backup & recovery, data labeling/retention, approved communications, secure file exchange.
- Continuous compliance: custom Security Assessment Checklist (monthly/quarterly).
- Evidence library structure: naming standards, screenshots, exports, tickets, change records, test results, training logs.

6) Audit-Ready Documentation (Month 7 — SSP development)

Authored and finalized the System Security Plan (SSP) with diagrams/data flows, inventories, and control narratives, linking each evidence artifact to its requirement.

7) Mock Assessment & Preparation (Month 8 — evidence & readiness)

Collected and linked artifacts, ran a full mock assessment with a CCA not previously exposed to the environment, corrected minor issues, and prepared the team for C3PAO interviews.

8) C3PAO Selection & Support

Advised on C3PAO options (availability, pricing, experience) and staffed the assessment with CCAs/CCPs to navigate interviews and evidence requests.

Results

- Certification: CMMC Level 2 achieved with 110/110.

- Speed: assessment fieldwork completed in a few days due to auditor-friendly evidence.
- Scope control: only essential users/systems/data flows included, lowering cost and risk.
- Operational practicality: enclave allowed business continuity with minimal disruption.
- Sustained compliance: continuous checklist and evidence library enable easy maintenance.

What We Implemented

- Access Control (AC): role-based access, least privilege, admin separation, periodic access reviews.
- Identification & Authentication (IA): MFA everywhere in scope; privileged credential lifecycle; service-account governance.
- Audit & Accountability (AU): centralized log retention; clock sync; admin-action alerting.
- Configuration Management (CM): baselines, change tracking, pre-deployment scanning; controlled admin tools.
- Incident Response (IR): IR plan & playbooks; tabletop exercise; escalation matrix and comms.
- Media Protection (MP): removable media restrictions; encryption; paper CUI handling and destruction.
- Physical Protection (PE): visitor controls; access device management; secure storage.
- Risk Assessment (RA): org risk register; treatment plans; leadership summaries.
- System & Information Integrity (SI): vuln scanning cadence; anti-malware; flaw remediation SLAs.

Why a COTS Secure Enclave Was the Right Choice

- High control coverage via inherited controls from a FedRAMP-authorized provider.
- Small user cohort reduced licensing and operational overhead vs. GCC-High or on-prem builds.
- Faster time-to-audit with pre-hardened services and proven evidence patterns.
- Predictable costs aligned to the client's monthly budget.

Risks of Non-Compliance

- Bid ineligibility: barred from DoD contracts requiring CMMC.
- Prime/sub risk: primes may drop non-compliant subs from opportunity lists.
- Revenue loss: missed bids and displaced subcontracting directly reduce pipeline.
- Contractual exposure: potential stop-work, termination, or damages.
- Reputational harm: signals weak security governance to customers and partners.
- Operational risk: higher probability of breaches, downtime, data loss, and costly incidents.

Timeline & Milestones

- Weeks 1–4: free consultation; scoping workshops; CUI data mapping; boundary definition.
- Weeks 3–6: solution analysis and selection; enclave provisioning; high-level gap assessment.
- Months 1–6: implement 30+ requirements per month; policies, controls, training; build the evidence library structure.
- Month 7: SSP development and finalization with diagrams, inventories, and narratives.
- Month 8: evidence collection and assessment preparation; mock assessment with a fresh CCA; C3PAO selection and scheduling.
- Assessment Week: evidence walkthrough; interviews; 110/110 achieved.

Artifacts Delivered

- System Security Plan (SSP) with data-flow diagrams and inventories.
- Policies & Standards: AC, IA, CM, IR, MP, PE, RA, SI; Alternate Work Site; Acceptable Use.
- Training & Acknowledgements: security awareness; user acknowledgement forms.
- Risk Management: enterprise risk assessment and risk register.
- Testing & Exercises: tabletop exercise with after-action report; vuln scan results; remediation tickets.
- Continuous Compliance: monthly/quarterly Security Assessment Checklist; evidence maintenance plan.

What Made the Project Succeed

- Right-sized scope limited to the departments that handle CUI.
- Inherited controls from the secure enclave accelerated compliance.
- Auditor-friendly evidence: one-click traceability from SSP → control → artifact.
- Independent peer review by a CCA prior to C3PAO engagement.
- Change management and cadence: ~30+ controls/month for six months, followed by month 7 SSP development and month 8 evidence/assessment prep.
- Budget-aligned pacing: we can work faster; the client chose a steady monthly investment. Early action (already handling CUI) removed deadline stress and avoided missed-bid risk.
- Co-managed delivery with the client's two IT pros and the MSP.

Why Hire A Cyber Pro

- Assessor-led team: CCAs and CCPs who understand what passes because we assess and build programs.
- Playbook, not guesswork: templates, evidence patterns, auditor-ready structures.
- Public- and private-sector depth across DoD subs, higher-ed, local government, and regulated industries.

- Flexible engagement models: fixed scope, phased remediation, vCISO support, co-managed delivery.
- Insured, veteran-owned partner focused on measurable outcomes.

Next Steps

- Book a free consultation to review contracts, timelines, and scope.
- Run a CUI scoping workshop to define boundaries and eliminate unnecessary scope.
- Decide on the right enclave path: COTS, GCC-High, or on-prem based on users and integrations.
- Execute the plan and implement your CMMC certified environment.
- Schedule a mock assessment, tune evidence, and select your C3PAO.

Conclusion

CMMC success is about disciplined scoping, smart solution choices, and repeatable execution, not heroics. By right-sizing the boundary, leveraging inherited controls, and pacing delivery to the client's budget, Hire A Cyber Pro helped this government contractor achieve **110/110** while protecting bid eligibility and revenue. If your organization handles FCI or CUI and wants a predictable path to **CMMC Level 2**, we can guide you from scoping and solution selection through implementation and evidence collection, mock assessments, and C3PAO support.

Contact Hire A Cyber Pro
Email: contact@hireacyberpro.com
Web: www.hireacyberpro.com
Book a free consultation to discuss scope, timelines, and the best-fit path to certification.