Case Study

FROM NIST 800-171 READINESS TO EARLY CMMC CERTIFICATION: PROACTIVE COMPLIANCE AS A COMPETITIVE ADVANTAGE

A case study on McAleese & ACTIVECYBER

McAleese AND ASSOCIATES

ACTIVECYBER

Moving before the requirement

For many companies in the defense industry, CMMC has remained a future problem. McAleese treated it as a business decision.

The engagement with ACTIVECYBER began with NIST 800-171, but leadership quickly recognized that waiting for the final rule would create risk. Assessment capacity will be limited. Contract timelines will not move. Companies that start late will be forced into reactive compliance under pressure.

Instead of slowing down, McAleese used the uncertainty in the market to build a structured, auditable security program aligned to CMMC Level 2.

The objective was clear.

Be ready for the assessment before it becomes a contract requirement.

Executive Summary

Building an assessable CMMC Level 2 program

ACTIVECYBER partnered with McAleese to turn an 800-171 effort into a security program that could stand up to a third-party assessment. The work focused on making the environment defensible, repeatable, and owned across the business, not just technically implemented.

Key objectives included:

- **Establishing a validated NIST 800-171 baseline that maps cleanly to CMMC Level 2**
- **Building the System Security Plan, POA&M discipline, and control ownership model**
- **Creating audit-ready evidence aligned to how a C3PAO performs an assessment**
- **Moving from project-based compliance to an operational program**
- **Positioning the organization for early entry into the C3PAO assessment queue**

CMMC stopped being a compliance discussion for us once we understood the assessment bottleneck that was coming. ACTIVECYBER fully designed our CMMC program the right way so we could get certified on our first pass. This early certification allows us to continue supporting mission-critical initiatives for the defense industry.

Jim McAleese, Esq., LL.M.

Principal, McAleese

Summary

Building a certification-ready program with the ACTIVE *Framework*™

The ACTIVE Framework™ gave McAleese a structured path from control implementation to full CMMC Level 2 assessment readiness.
Each phase focused on making the program operational, owned, and supportable under audit conditions.

ACTIVE

Advisory

Established a defensible 800-171 baseline and defined the gap to CMMC Level 2 at the practice and process level.

Compliance

Formalized policies, procedures, and technical controls so they function consistently and can be demonstrated during an assessment.

Testing

Performed resiliency testing and mock assessment activities using real C3PAO expectations to validate readiness and identify breakdowns early.

Implementation

Built the System Security Plan, POA&M management process, and evidence model around how the environment actually operates.

Visibility

Confirmed control ownership across the business and prepared stakeholders to support the assessment process.

Education

Positioned the program for certification on McAleese's timeline, with a structure that can be maintained as requirements mature - including ongoing training to employees.

The Approach

Building readiness before the market rush

- **Starting with 800-171 as the foundation**: Control implementation was stabilized first. The System Security Plan, POA&M process, and supporting documentation were aligned to how the environment actually operates.
- **Mapping to CMMC Level 2 early:** Existing controls were evaluated against CMMC Level 2 practices and processes so the program could mature without waiting for the final rule.
- **Designing for a real assessment**: Evidence collection, control ownership, and documentation were structured around how a C3PAO performs an audit, not around a checklist.
- **Operationalizing control ownership**: Responsibility for controls moved out of a central compliance function and into the teams that run the environment day to day.
- **Securing a place in the assessment queue**: By reaching readiness early, McAleese was able to plan for certification ahead of the capacity constraints that will impact late movers.

Impact & Outcomes

Assessment timeline under control

Because the environment, documentation, and control ownership are already aligned to CMMC Level 2, McAleese moved into certification without a last-minute rebuild.

Early position with a C3PAO

Planning for assessment began before the market surge, avoiding the scheduling constraints late adopters will face.

Stronger standing with primes and partners

Cybersecurity maturity can be demonstrated today through an auditable program, not a future roadmap.

Reduced certification risk

Mock assessment activity and structured evidence development removed uncertainty from the path to audit.

McAleese's approach reflects where the defense industry should be heading. Organizations that wait for CMMC to appear in a contract will be forced to move on someone else's timeline. Proactive readiness changes the conversation from compliance to capability.

Dale A. Raymond
ACTIVECYBER Founder & CEO

ACTIVECYBER

PROVE YOU'RE SECURE

DEMONSTRATE COMPLIANCE

MAINTAIN TRUST

For more information, visit us at activecyber.us or contact info@activecyber.us

ACTIVECYBER