CMMC Advisors

CMMC Implementation Update

A comprehensive overview of the Cybersecurity Maturity Model Certification (CMMC) program implementation, key requirements, and strategic guidance for defense contractors navigating the evolving compliance landscape.

Jerry Leishman. CEO
October 28, 2025

INTRODUCTIONS

Jerry Leishman

CEO – CMMC Advisors

jerryleishman@cmmcadvisors.com

206-484-9936

www.cmmcadvisors.com

Jerry serves as a trusted advisor to in-house counsel, compliance officers, and senior executives, assisting them in managing complex regulatory, legal, and contractual risks and responsibilities.

He currently is **CEO of CMMC Advisors**, based in Seattle providing support to a wide array of Defense and Critical Infrastructure suppliers to strengthen their cybersecurity resilience.

Previously, Jerry held the position of **EVP at CORTAC Group** and **Microsoft**. His extensive experience in national cybersecurity and compliance includes roles such as:

- Plank Member of the CMMC Accreditation Body Standards Workgroup (recipient of the Presidential Volunteer Service Award),
- Vice-Chair of the CMMC Industry Standards Council (CISC),
- Provisional and Certified CMMC Assessor (PA, CCA),
- Certified CMMC Professional (CCP) and Registered Practitioner (RP),
- Co-Chair of the Software for Defense nonprofit.

Jerry is a regular speaker at national events, advising Defense Industrial Base (DIB) leaders on cybersecurity and DFARS/CMMC compliance. He helps executives recognize their essential role in protecting relationships with customers, partners, suppliers, and government entities. His strong connections within the CMMC community and leading technology providers enable him to deliver top-tier solutions for the Defense Supply Chain.

GOALS

Understand CMMC

Grasp the framework at a high level for effective leadership.

Planning and Implementation

Understand the CMMC Journey and Steps to get Certification.

Budgeting

Develop roadmaps for CMMC budgeting and compliance.

New Opportunities

ROI of CMMC security & compliance investments

CMMC Implementation Begins November 10, 2025

The Cybersecurity Maturity Model Certification (CMMC) program officially **launches on November 10, 2025,** marking a critical milestone for defense contractors and the broader defense industrial base. This comprehensive cybersecurity framework will fundamentally transform how **Defense Industrial Base (DIB) organizations internal systems & their external service providers (people, process, & technology),** handle controlled unclassified information (CUI) and federal contract information (FCI).

CMMC: A Tale of Two Rules:

- **32 CFR Part 170 (CMMC Program)** - Establishes the CMMC program framework for FCI/CUI protection
- **48 CFR (DFARS 252.204-7021)** - Implements CMMC requirements into contract language for DoD

Does CMMC Apply to Photo Chemical Machining Industry?

Understanding Your Compliance Requirements in Defense Manufacturing

If your company provides parts, services, or support for Department of Defense (DoD) contracts—even indirectly—you may be required to comply with the Cybersecurity Maturity Model Certification (CMMC). This federal requirement is reshaping how manufacturers across the defense supply chain approach data security and compliance.

Mandatory for DoD Contractors

CMMC compliance is now required for all DoD contractors and subcontractors, including manufacturers who produce components for defense-related applications. This requirement extends throughout the entire supply chain, even if you're a tier-2 or tier-3 supplier operating several steps removed from the prime contractor.

PCM in Defense Applications

Photo chemical machining is frequently used in aerospace, electronics, and defense sectors. If your precision-etched parts are incorporated into military systems, avionics, guidance systems, or secure communications equipment, you're likely handling **Controlled Unclassified Information (CUI)**, which automatically triggers CMMC requirements.

🔍 Key Considerations for PCM Shops

Who Must Comply

- **All tiers of suppliers** who handle CUI or participate in defense contracts
- Small shops and precision manufacturers processing technical drawings or specifications
- Companies storing, transmitting, or processing any defense-related technical data
- Subcontractors working with prime contractors on DoD programs

Limited Exemptions

- Commercial-off-the-shelf (COTS) suppliers providing unmodified standard products
- Vendors supplying publicly available commercial items without customization
- **Note:** Most custom or precision manufacturers producing to specifications do not qualify for exemptions

Bottom Line: If you manufacture custom photo-chemically machined parts for customers in the defense sector, or if you receive technical drawings, CAD files, or specifications marked as CUI, CMMC Level 2 compliance is likely required for your business. Non-compliance can result in lost contracts and exclusion from the DoD supply chain.

THE CMMC MODEL & ASSESSMENT REQUIREMENTS

FCI Definition

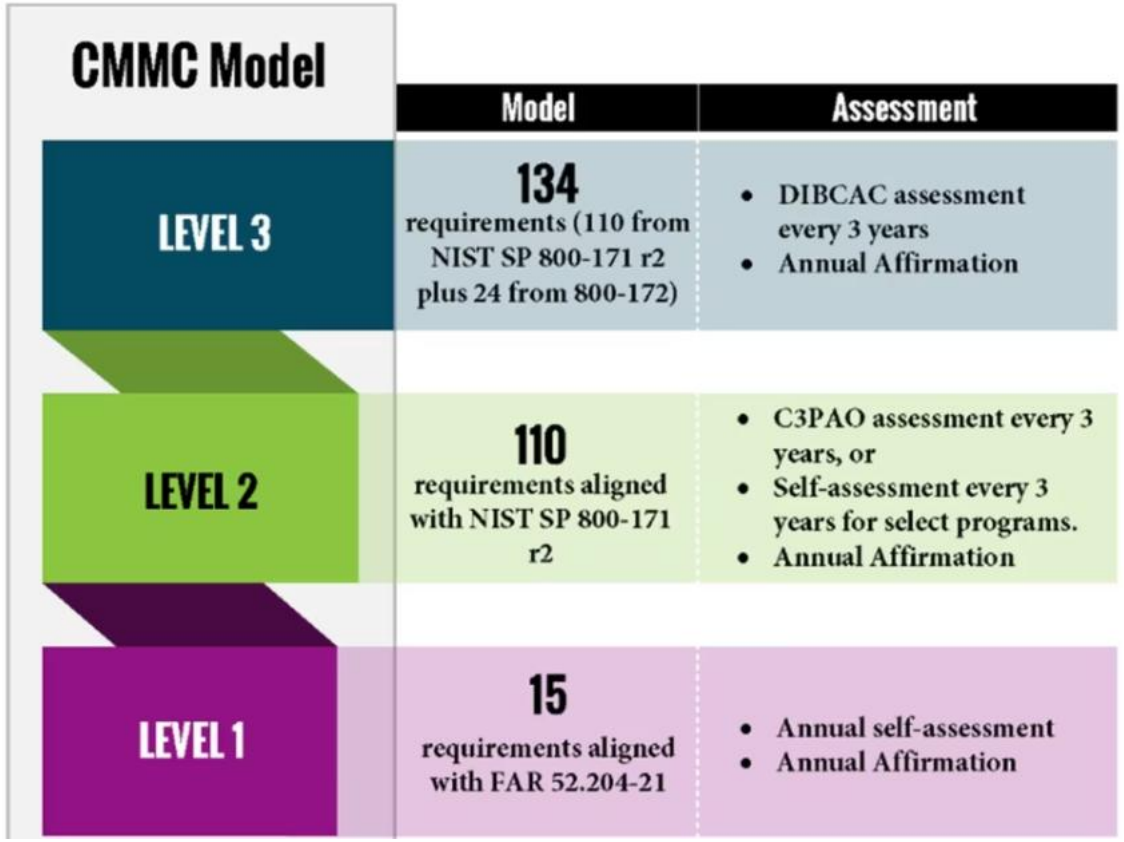
Contract Information - Any non-public, unclassified government information provided by or generated for the government under a contract, regardless of format or medium.

CUI Definition

Technical Information - Non-public, unclassified information stored, transmitted or created for or on behalf of the federal government where law, regulation, or government-wide policy requires safeguarding or limits dissemination.

COTS

Off-The Shelf - Commercially available Product (Out of Scope)



Critical Insight: DoD Program Data drives both the CMMC Model selection and Assessment Requirements. Understanding your data classification is the foundation of CMMC compliance

ROLLOUT TIMELINE

STAGE	DATE	REQUIRED	OPTIONAL	PMO APPROVAL REQUIRED
1	11/10/25	L1 (Self) and L2 (Self) requirements in all applicable DOW solicitations and contracts	• L1 and L2 self-assessments required at option period for previously awarded contracts • L2 C3PAO Condition or Final Certification required as a condition of award	YES
2	11/10/26	Phase 1 + Level 2 (C3PAO) requirements in all applicable DOW solicitations and contracts	• L3 DIBCAC Conditional or Final Certification required as a condition of award • May delay L2 C3PAO Conditional or Final Certification requirement until option period	YES
3	11/10/27	Phase 2 + Level 3 (DIBCAC) requirements in all applicable DOW solicitations and contracts. Level 2 (C3PAO) required to exercise option period	• May delay L3 DIBCAC Conditional or Final Certification requirement until option period	YES
4	11/10/28	Full implementation of CMMC program requirements in all DOW solicitations and contracts including option periods	• None	NO

Authority Notice: Contracting Officers maintain authority to require Conditional or Final Certification, or mandate a C3PAO audit at any time, regardless of the general rollout timeline.

CMMC IS A 5 STEP JOURNEY

1

Gap/Self-Assessment

Evaluate current CUI boundary against all 110 NIST SP 800-171 security controls to identify compliance gaps. ***(update SPRS Score)***

2

Remediation Planning

Develop detailed implementation plan to address identified gaps with specific timelines and resource allocation

3

Implementation

Deploy technical controls and establish process documentation across all 14 security control families

4

Pre/Mock-Assessment

Conduct comprehensive internal assessment with evidence collection for all 320 assessment objectives

5

Self or C3PAO Assessment

Engage a C3PAO to do your certification assessment ***(Update SPRS Score)***

IDENTIFY YOUR BOUNDARY & GAPS

Stakeholder & Data Mapping

Identify key stakeholders, all data sources, and systems that handle FCI/CUI. Map data flows and understand how information moves throughout your organization.

Workflow Analysis

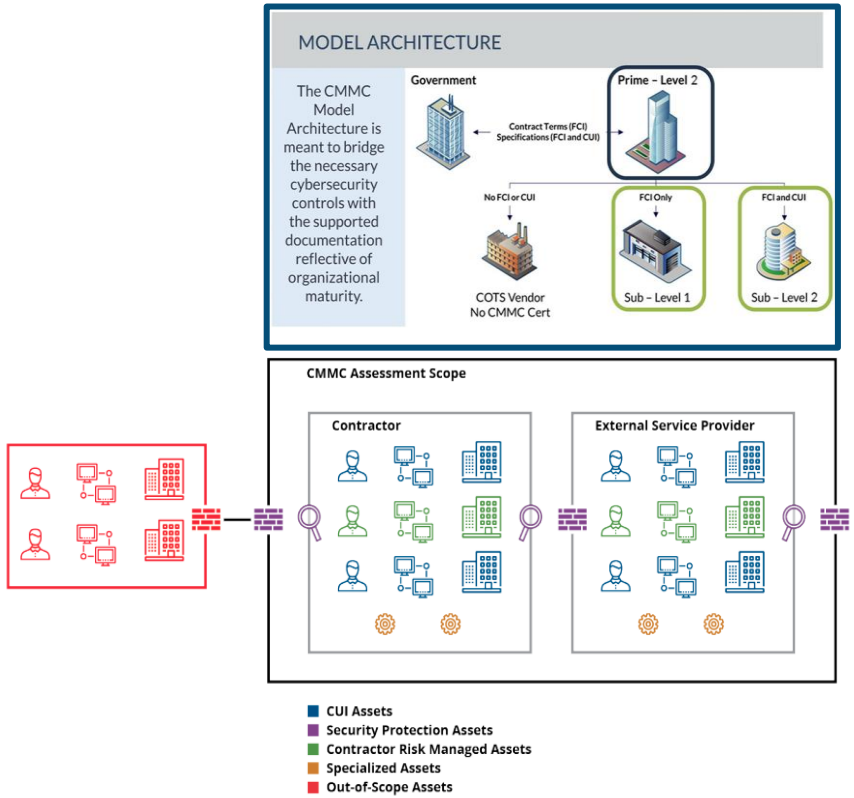
Review internal and external workflows to subcontractors and External Service Providers (ESP). Document all touchpoints where FCI/CUI is processed, stored, or transmitted.

Service Provider Assessment

Identify Internal/External Service Providers including Shared Services, Cloud Service Providers (CSP), Managed Service Providers (MSP), and Managed Security Service Providers (MSSP). Define shared responsibilities for security controls.

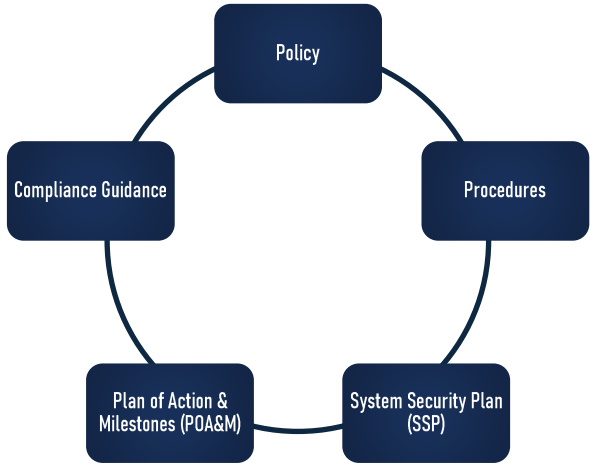
Gap Analysis & Scoring

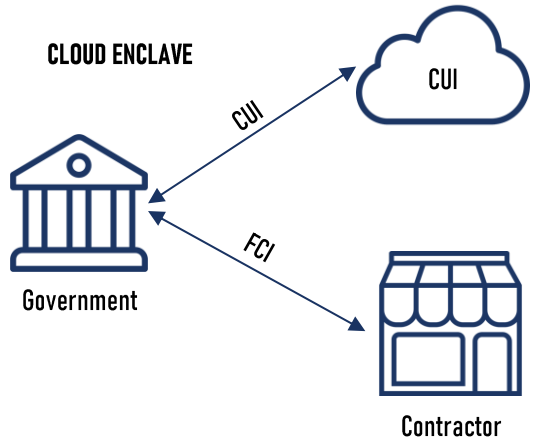
Identify compliance gaps against NIST SP 800-171 requirements and calculate current SPRS score based on actual implementation status.

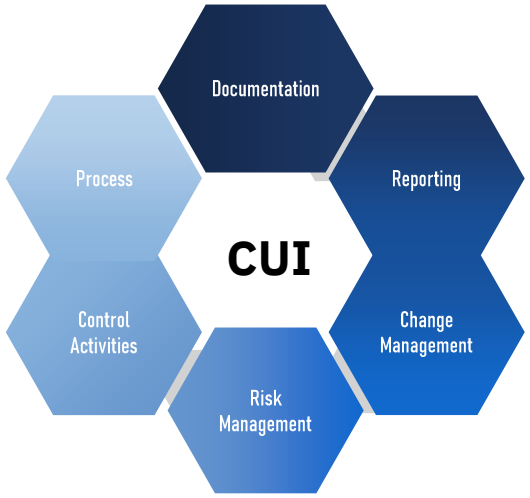


Best Practice: The most effective way to protect FCI/CUI is to minimize collection and limit where it is stored and transmitted throughout your organization.

GAP MITIGATION AND IMPLEMENTATION







Documentation

- Policies
- Procedures
- System Security Plan (SSP)
- Implementation Plan, Timeline, Budget

Technical Solutions

- CUI isolation
- On-Premise/ESP enclave
- ESP Shared Responsibilities
- End point Protection

Governance, Risk & Compliance

- Control activities
- POA&M management
- Risk management
- Change processes

Best Practice: Documentation, Processes, Evidence, & Systems must match the System Security Plan (SSP)

C3PAO LEVEL 2 ASSESSMENT

01 Preparation Phase

1-2 weeks

- Documentation review & validation
- Contract signature

02 Assessment Execution

2-4 weeks

- Onsite & offsite interviews
- Testing and validation

03 Results & Reporting

2-4 weeks

- Assessment results determined
- MASS system updates

Possible Outcomes (Self & C3PAO)

Failed - SPRS score < **88** (Reassessment required)

Conditional - SPRS Score > **88** & ALL Mandatory Controls (180 Remediation)

Final - SPRS Score **110** (perfect) - 3-year recertification

Lead Time Planning

Minimum 90 days lead time required

High demand, limited assessor availability

Investment Range

$30K to $100K+ assessment costs

Based on complexity, scope, objectives

Contract Eligibility

Both Conditional & Final status

Enable contract awards requiring CMMC

Estimated CMMC Level 2 Cost Model

Understanding the full financial investment required for CMMC Level 2 certification is critical for strategic planning and budget allocation. This comprehensive cost model breaks down Year 1 implementation and ongoing maintenance expenses.

Year 1 Implementation Investment Breakdown

CUI Boundary Discovery & Planning	$15,000 - $50,000	CUI discovery, scoping analysis, comprehensive CMMC gap assessment
Gap Remediation/Implementation/Tools	$25,000 - $300,000	Documentation, technology deployment, governance frameworks, staff training
Pre-Assessment & Verification	$5,000 - $20,000	Internal/External CMMC readiness validation (RPO, C3PAO mock assessment)
C3PAO Official Assessment	$30,000 - $80,000	Third-party certification assessment by Authorized C3PAO

$75K-$450K+

Total Year 1 Investment

Complete implementation from assessment through certification

$50K-$150K+

Years 2-3 Annual Maintenance

Ongoing CMMC operations, monitoring, and yearly affirmation requirements

Implementation Costs Will Vary: Actual costs vary significantly based on organization size, existing security maturity level, scope of current CUI environments, utilization of External Service Providers, complexity of technical environment, and desired timeframe for achieving certification. Organizations with mature cybersecurity programs may see costs at the lower end of ranges, while those starting from baseline may require investments at the higher end.

The Global Defense Market: A Trillion-Dollar+ Opportunity

$1T+

Annual Global DIB Spending

The global Defense Industrial Base sector represents over **$1 trillion in annual spending**, supporting R&D, design, production, and maintenance of military systems and critical defense technologies.

Greatest Opportunity in Your Lifetime!

Key Market Dynamics

Billions in Revenue Opportunity

Federal cybersecurity mandates reshape the market—creating risks for unprepared organizations and opportunities for capable providers.

Rising Investment Requirements

Defense suppliers are increasing investments, with CMMC Level 2+ compliance often driving security spend to **5–6% of revenue** during peak years.

Massive Addressable Market

Estimated 300K+ contractors and 2.5M federal vendors. CMMC certification unlocks high-value contracts across defense and civilian agencies.

Compliance Gap: Gartner reports regulated industries spend **6-10%** of revenue on IT, cybersecurity, and compliance. Defense currently allocates only **2-4%**—creating a significant capabilities gap.

When the Federal Government Changes the Rules, there are new winners and losers!

Strategic Opportunities for CMMC Level 2 Suppliers

Achieving CMMC Level 2 certification offers significant competitive and financial advantages for defense contractors, positioning you as trusted partners for sensitive defense information.

Eligibility for CUI Contracts

Level 2 certification is **required for contracts involving Controlled Unclassified Information (CUI)**, making suppliers eligible for higher-value and longer-term agreements.

Preferred by Prime Contractors

Major defense primes like **Boeing and Lockheed Martin** increasingly require Level 2, signalling trustworthiness and operational maturity for multi-tiered supply chains.

Competitive Differentiation

Early adopters gain market advantages, as CMMC becomes a **critical differentiator**. Compliant organizations win contracts over non-compliant competitors.

Access to Strategic Programs

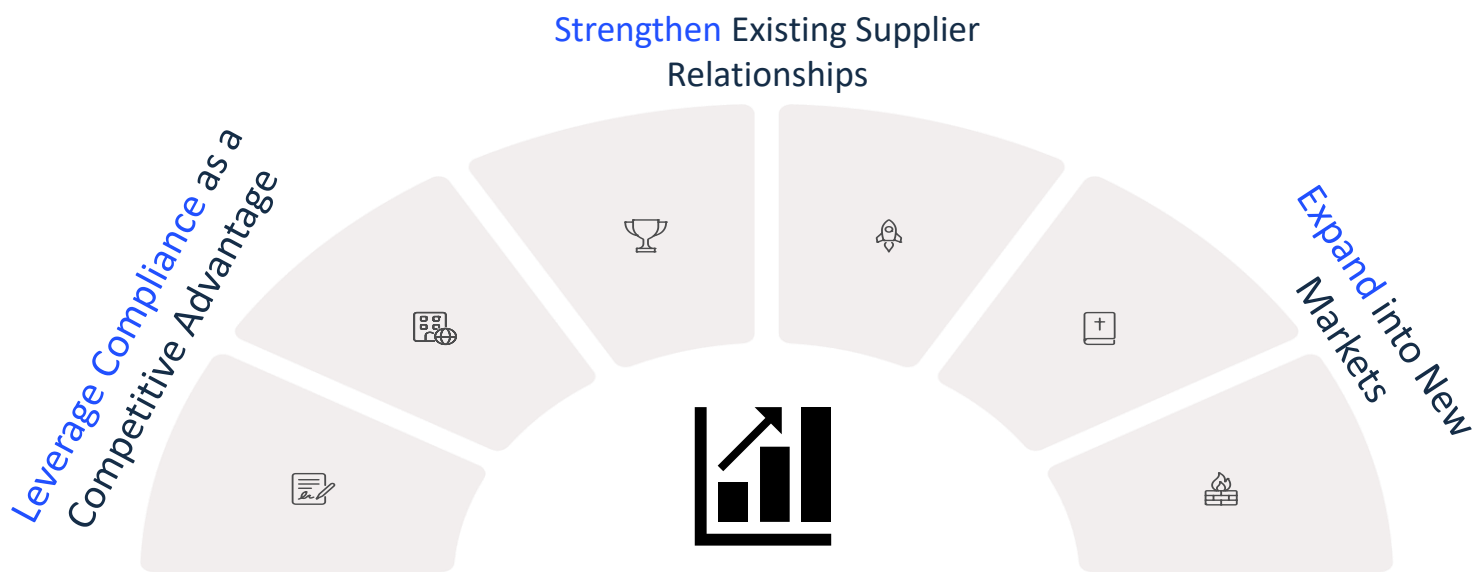
Level 2 suppliers can compete for contracts involving **classified prototypes, R&D, and next-generation platforms** like the F-35 fighter, where cybersecurity is mission-critical.

Reduced Risk of Contract Loss

CMMC Level 2 will be a hard requirement by **2026-2028**. Certification helps avoid disqualification, contract termination, and loss of revenue streams.

Enhanced Cyber Resilience

Beyond compliance, Level 2 leads to **stronger internal security architectures**, reducing risks of data breaches, ransomware attacks, and reputational damage.



Case Study: Aero-Glen International

CMMC 2.0 Certification & Wencor Acquisition

Aero-Glen Business Focus

Founded in 1976, **Aero-Glen at $16M** specializes in aerospace fasteners and supply chain services for diverse clients.

1

CMMC 2.0 Compliance

Compliance with CMMC 2.0 Level 2 was critical to retain and compete for Department of Defense contracts.

2

Successful Certification

Aero-Glen was **first in the US** to complete the Joint Surveillance Voluntary Assessment in 2023 with minor findings.

3

Strategic Acquisition

Wencor, $155M defense supplier, acquired Aero-Glen in 2023 to expand aerospace supply chain and enhance value-added services.

4

CMMC Level 2 Executive Action Plan

Phase	Executive Actions	Strategic Focus
1. Ownership & Governance	• Appoint CMMC Program Lead • Form cross-functional steering committee • Set certification timeline	Accountability & enterprise alignment
2. CUI Scope Definition	• Map CUI data flows • Segment systems • Visualize boundary	Audit clarity & control scoping
3. Maturity Assessment	• Conduct NIST SP 800-171 gap analysis • Score SPRS readiness • Prioritize high-risk domains	Risk visibility & remediation planning
4. Technology Modernization	• Rationalize cyber tools • Secure cloud environments • Enforce MFA & RBAC	Control maturity & audit readiness
5. Supply Chain Compliance	• Build supplier risk matrix • Update contracts with flowdowns • Launch vendor enablement program	Ecosystem assurance & flowdown enforcement
6. Cultural Alignment	• Deliver role-based training • Frame CMMC as mission-critical • Model executive commitment	Behavioral adoption & sustained compliance
7. Assessment Preparation	• Conduct mock interviews • Standardize documentation • Engage certified C3PAO	Audit success & certification confidence
8. Sustainment & Monitoring	• Build compliance dashboard • Schedule quarterly reviews • Plan for recertification	Long-term resilience & contract eligibility

Key Success Factors

- **Executive Leadership**

  Educate and engage C-suite and board members on CMMC strategic importance and business impact

- **Workforce Strategy**

  Determine optimal balance of hiring internal expertise versus engaging external consultants and service providers

- **Build vs. Buy Decisions**

  Evaluate technology solutions strategically based on organizational capabilities, timeline constraints, and total cost of ownership

- **Collaboration Approach**

  Balance speed of independent action with benefits of industry collaboration and shared learning opportunities

RESOURCES

Templates and Examples

- CMMC Level 1 Scoping Guidance: CMMC Level 1 Scoping Guidance
- CMMC Level 1 Self-Assessment Guide: CMMC Level 1 Self-Assessment Guide
- CMMC Level 2 Scoping Guidance: CMMC Level 2 Scoping Guidance
- CMMC Level 2 Assessment Guide: CMMC Level 2 Assessment Guide
- CMMC mapping template
- CMMC Assessment template
- CUI System Security Plan Template
- CMMC Assessment Scoring Template
- CMMC Detailed Assessment Template
- Example Policy Template
- Tasks to maintain CMMC Compliance Template

Documentation and References

- DoD CIO Home page for Cybersecurity Maturity Model Certification
- Official DoD CIO CMMC Resources & Documentation website
- DoD CUI Program website
- 32 CFR Part 170: Cybersecurity Maturity Model Certification Program
- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-171 Rev. 2: Protecting CUI in Nonfederal Systems
- NIST SP 800-171A: Assessing Security Requirements for Controlled Unclassified Information
- DoD Procurement Toolbox: Implementing the Cybersecurity Maturity Model Certification (CMMC) Program

Thank You

Jerry Leishman - CEO

jerryleishman@cmmcadvisors.com

206-484-9936

www.cmmcadvisors.com

CMMC Advisors Comprehensive Services

Executive and CMMC Training

Comprehensive workshops and training programs for executives, project teams, and technical staff to build organizational CMMC expertise and readiness.

CMMC Implementation Projects

End-to-end support including CUI discovery, gap assessments, remediation implementation, documentation development, and ongoing virtual CISO operational support.

CMMC In A Box Solution

Integrated turnkey solution combining hardware, software, governance frameworks, comprehensive documentation, and professional services for rapid deployment.

Cybersecurity Advisory Services

Monthly cybersecurity and compliance advisory services providing ongoing strategic guidance, regulatory updates, and continuous improvement support.

CMMC Advisors is deeply committed to helping defense contractors and suppliers achieve sustainable cybersecurity compliance. Our comprehensive approach strategically combines expert guidance, technical implementation support, governance frameworks, and ongoing advisory services to ensure your organization is fully prepared for CMMC requirements.

Contact us today to discuss your specific CMMC needs and develop a customized compliance strategy that protects your business while meeting all federal cybersecurity requirements and positioning your organization for competitive advantage.