Securing Defense Information: CMMC 2.0's Impact on Cybersecurity Requirements

By Frank Balonis

The Department of Defense has established a critical one-two regulatory punch for protecting sensitive defense information through its Cybersecurity Maturity Model Certification 2.0 Program. The first component, 32 CFR Part 170, takes effect December 16, 2024, with the second component, 48 CFR Part 204, following in 2025. This coordinated regulatory approach addresses a stark reality: malicious cyber activity costs the U.S. economy between $57 billion and $109 billion annually, with the defense industrial base facing persistent targeting from sophisticated threat actors.

The Council of Economic Advisors calculates these attacks could burden the U.S. economy with up to $1.09 trillion in costs over a decade. To combat this threat, CMMC 2.0 creates new requirements for more than 220,000 defense contractors who process, store, or transmit sensitive defense information. 32 CFR Part 170 establishes the program structure and security standards, while 48 CFR Part 204 implements contractual mechanisms through the Defense Federal Acquisition Regulation Supplement.

Three-Year, Four-Phase Implementation for Defense Contractors

CMMC 2.0 establishes three distinct control levels based on information sensitivity. Level 1 requires 15 basic cybersecurity controls from FAR 52.204-21 for protecting Federal Contract Information, focusing on fundamental practices like access control and basic system security. Level 2 mandates all 110 security requirements from NIST SP 800-171 Rev 2 for protecting Controlled Unclassified Information, encompassing comprehensive controls across 14 domains including access control, incident response, security assessment, and system integrity. Organizations must achieve a minimum score of 88 out of 110 points. Level 3 builds upon Level 2 by requiring a perfect score of 110 on NIST SP 800-171 Rev 2 controls plus 24 additional enhanced security requirements from NIST SP 800-172, including advanced threat monitoring, 24/7 security operations center capabilities, and cyber incident response teams that can deploy within 24 hours.

The DoD's implementation strategy spans four distinct phases over three years:

- **Phase 1: Initial Implementation**
- Begins at 48 CFR Rule Effective Date.
- Where applicable, solicitations will require Level 1 or 2 Self-Assessment.
- DoD estimates 1,104 small businesses will participate in this initial phase, allowing organizations to adapt to new requirements while limiting broader impact.

- **Phase 2**
- Begins 12 months after Phase 1 start.
- Where applicable, solicitations will require Level 2 Certification with assessments conducted by CMMC Third Party Assessment Organizations (C3PAOs).
- Projected 673 C3PAO certifications during this phase, enabling the assessment ecosystem to mature methodically.

- **Phase 3**
- Begins 24 months after Phase 1 start.
- Where applicable, solicitations will require Level 3 Certification.
- During this phase, DoD projects completion of 2,252 C3PAO certification assessments.

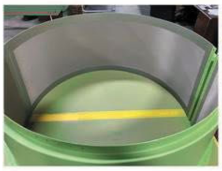
- **Phase 4: Full Implementation**
- Begins 36 months after Phase 1 start.
- All solicitations and contracts will include applicable CMMC Level requirements as a condition of contract award.
- Annual C3PAO assessments will reach 4,452, covering approximately 20,395 small entities and 9,148 large entities.

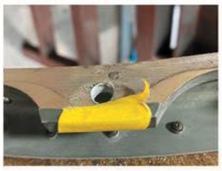
Understanding the CMMC 2.0 Certification Verification Process

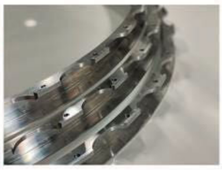
CMMC certification scoring varies by level, with each tier requiring progressively more rigorous verification by C3PAOs. Level 1 employs a straightforward met/not-met scoring system for its 15 basic safeguarding requirements from FAR 52.204-21. For Level 2, organizations must achieve a minimum score of 88 out of 110 possible points based on NIST SP 800-171 Rev 2 security requirements, while Level 3 demands a perfect Level 2 score plus successful implementation of 24 additional enhanced security requirements from NIST SP 800-172.

C3PAOs, accredited by the CMMC Accreditation Body, serve as the primary assessors for Level 2 certifications, conducting comprehensive evaluations that have replaced the previous self-attestation model. During assessments, C3PAOs examine both technical implementations and organizational processes, including detailed reviews of system configurations, security policies, operational procedures, and control implementations. The assessment process includes documentation review, system testing,

WINGLETS
FLAPS
SPOILERS
AILERONS
ELEVATORS
RUDDERS
WING TIPS
ACCESS PANELS
INLETS
FAN COWL DOORS
THRUST REVERSERS
FAIRINGS
DOOR ASSEMBLIES
RADOMES







personnel interviews, and direct observation of security practices.

The CMMC Accreditation Body maintains oversight of C3PAOs by establishing assessment standards, monitoring performance, and ensuring consistent evaluation methodologies. Additionally, the Defense Industrial Base Cybersecurity Assessment Center provides another layer of quality control by conducting regular evaluations of C3PAO capabilities and performing high-priority assessments. Organizations seeking certification must submit assessment results and maintain current status in the Supplier Performance Risk System, with a senior company official required to affirm continued compliance annually or when security changes occur. If deficiencies are identified during assessment, organizations may achieve conditional certification through Plans of Action and Milestones (POA&Ms), which must address permitted gaps within 180 days.

180-Day Conditional Certification Pathway for Addressing Security Gaps

CMMC 2.0 permits limited use of Plans of Action and Milestones (POA&Ms) for Level 2 and 3 certifications. Organizations meeting minimum scoring requirements can achieve conditional certification by addressing permitted deficiencies within 180 days. This flexibility supports transition while maintaining security standards. POA&Ms must address specific remediation timelines, resource requirements, and technical solutions for each identified gap.

Governance and Supply Chain Obligations

The regulations establish clear contractual implications through 48 CFR Part 204, expected to be published in 2025. Contractors must achieve their required CMMC level before contract award. Contracting officers cannot award contracts, exercise options, or extend performance periods without verification of current certification. Prime contractors must validate subcontractor compliance based on the sensitivity of information in the supply chain, ensuring security requirements flow down appropriately.

The certification ecosystem includes several oversight components. The CMMC Accreditation Body establishes assessment standards and monitors C3PAO performance. The Cybersecurity Assessor and Instructor Certification Organization manages training programs and maintains certification standards. The Defense Industrial Base Cybersecurity Assessment Center conducts high-priority assessments and validates C3PAO capabilities through regular evaluations.

Oversight Framework

Organizations must submit assessment results and maintain current status in the Supplier Performance Risk System. A senior company official must affirm continued compliance annually or when security changes occur. The DoD requires current certification or self-assessment results for each contractor information system processing sensitive defense information, with specific documentation requirements for system boundaries and security implementations.

CMMC 2.0's dual regulatory framework creates comprehensive cybersecurity enhancement across the defense industrial base. The phased implementation balances security imperatives with practical considerations about industry readiness and assessment capacity. As both regulations take full effect, they establish increasingly robust protection for sensitive defense information while maintaining supply chain vitality. Organizations must prepare now for these mandatory requirements, understanding that certification will soon determine their ability to compete for defense contracts involving protected information. AM

Frank Balonis is chief information security officer and senior VP of operations and support at Kiteworks, with more than 20 years of experience in IT support and services. Since joining Kiteworks in 2003, Balonis has overseen technical support, customer success, corporate IT, security and compliance, collaborating with product and engineering teams. He holds a Certified Information Systems Security Professional (CISSP) certification and served in the U.S. Navy. He can be reached at fbalonis@kiteworks.com.

10 Compliance Essentials for Cybersecurity and Data Protection

In today's complex regulatory environment, organizations must keep pace with diverse, often stringent security and privacy requirements. Here are 10 key compliance areas companies should prioritize to bolster defenses and reduce regulatory risks:

1. **Navigate Complex Regulations:** *Regulatory landscapes, including GDPR and HIPAA, demand strict data protections tailored by industry and region, requiring continuous monitoring and adaptation.*
2. **Create a Data Inventory and Classification System:** *Establishing a detailed inventory helps identify and categorize sensitive data, allowing for targeted protections across data life cycles.*
3. **Adopt Strong Data Protection Practices:** *Implement technologies like encryption and access controls to secure data during storage and transfer, essential for compliance and security.*
4. **Manage Third-Party Risks:** *Mitigate vulnerabilities introduced by vendors through thorough due diligence, routine security audits, and compliance monitoring.*
5. **Develop Incident Response Plans:** *Ensure rapid response to data breaches, with protocols for regulatory notification, containment, and recovery in line with GDPR's 72-hour rule and other timelines.*
6. **Follow Data Retention and Deletion Guidelines:** *Set policies for retaining data only as long as necessary and securely deleting outdated information to reduce exposure and meet legal requirements.*
7. **Promote Cybersecurity and Privacy Awareness:** *Regular training sessions raise awareness among employees, emphasizing the importance of protecting sensitive data and following compliance best practices.*
8. **Enhance Cyber Resilience:** *Develop business continuity and disaster recovery plans to sustain operations during cyber incidents, incorporating regular drills to test and improve resilience.*
9. **Maintain Governance Through Audits and Reporting:** *Routine audits and transparent reporting practices bolster governance, helping organizations demonstrate compliance and refine security protocols.*
10. **Follow a Comprehensive Compliance Checklist:** *Use a regulatory checklist to stay proactive, addressing specific regulations like CMMC 2.0, ensuring continuous improvement in compliance and security readiness.*

Space Logistics Network

A division of Aviation Logistics Network

We put the Space into Aerospace

Space Logistics Network is a specialist group of world leading companies dedicated to supporting the global aerospace industry.

We are unique in that we can offer a total end to end solution from production through to launch for logistical, transportation and specialist customs and supply chain engineering requirements.

Our service offering includes:

- Supply chain co ordination
- Specialist packing and asset tracking
- Customs Brokerage and facilitation
- Freight Forwarding
- Aircraft Charter
- Air Ride Trucking
- Insurance
- Engineering and Design

www.spacelogisticsnetwork.space

MRO

CFM MRO turns more than just wrenches.

It also turns heads in the boardroom. Our open, competitive MRO ecosystem is unique in the industry because it gives you choice. You decide where to overhaul your LEAP engines, meaning competitive pricing and more flexibility. Another reason to say **LEAP. By example.**

cfmaeroengines.com

An open, competitive MRO ecosystem.

LEADERS AREN'T BORN. THEY'RE ENGINEERED.