

Navigating the Complexities of CMMC 2.0 Compliance

The rise in targeted and sophisticated cyberattacks across the U.S. Department of Defense's (DoD) vast attack surface has precipitated the need to safeguard sensitive information that supports the warfighter. Securing third-party systems and remediating supply chain vulnerabilities has never been more critical. In November 2020, the DoD published an interim rule (DFARS Case 2019-D041) establishing the foundation for the Cybersecurity Maturity Model Certification (CMMC 2.0). The CMMC program aims to secure sensitive unclassified information or controlled unclassified information (CUI) shared by the DoD with its contractors and subcontractors by ensuring Defense Industrial Base (DIB) partners meet required cybersecurity standards.

The stakes have gotten higher as DIB partners are expected to comply with CMMC 2.0 by July 2025 or risk not being able to compete for DoD business. The DoD estimates it has approximately 220,000 companies in its industrial base, counting both prime contractors and their subs. Approximately 140,000 will need self attestation in order to achieve a Level 1 certification. Contractors seeking to achieve Level 2 or 3 will need to also undergo assessments by third-party organizations.

CrowdStrike is committed to enhancing its customers' security capabilities by fully supporting CMMC 2.0 as a vital certification for strengthening the cybersecurity posture of the U.S. DIB. CrowdStrike's suite of solutions meets rigorous government security requirements, including DoD Impact Level 5 (IL5) and Federal Risk and Authorization Management Program (FedRAMP) authorization. Whether you're a large systems integrator managing multiple contracts or a service-disabled veteran-owned small business navigating government procurement, CrowdStrike is here to support you at every stage of your CMMC 2.0 journey.

The CMMC 2.0 Journey

CMMC 2.0 aligns with the DoD's cybersecurity requirements for DIB partners, ensuring they meet the necessary standards for protecting sensitive unclassified information shared in acquisition programs and systems.

Key goals of CMMC include:

- Protecting sensitive information to enable and support warfighters
- Enforcing DIB cybersecurity standards in response to evolving threats
- Ensuring accountability and reducing compliance barriers for DoD requirements
- Fostering a collaborative culture of cybersecurity and resilience
- Maintaining public trust through professional and ethical standard

What to Know: Meeting CMMC 2.0 Compliance

DIB contractors must address requirements to meet CMMC 2.0 compliance by July 2025. Here are some of the top issues they face:

- **Navigating Compliance Requirements:** Many contractors struggle to fully understand the specific requirements of CMMC 2.0, especially as it involves different levels of compliance based on the sensitivity of the information they are entrusted to protect.
- **Cost Management:** Implementing the necessary cybersecurity measures can be expensive. Smaller contractors may find it difficult to allocate the required resources for compliance.
- **Sustainable Policy Implementation:** Developing and maintaining sustainable cybersecurity policies that meet CMMC 2.0 standards is a significant challenge. This includes continuous monitoring and updating of security practices.
- **Third-Party Assessments:** Contractors need to undergo assessments by third-party organizations in order to achieve higher levels of CMMC 2.0 compliance. This can be a complex and time-consuming process.
- **Cybersecurity Infrastructure:** Many contractors need to upgrade their existing cybersecurity infrastructure to meet the new standards. This includes implementing multifactor authentication, vulnerability management and other advanced security measures.
- **Risk of Non-Compliance:** Failure to comply with CMMC 2.0 can result in disqualification to compete for DoD contracts, which is a significant risk for most contractors.

These issues highlight the need for thorough preparation and investment in cybersecurity to meet the upcoming compliance deadline.

Preparing for CMMC 2.0 Assessments

Preparing for CMMC 2.0 assessments involves several key steps to ensure compliance and readiness:

- **Understand the Requirements:** Familiarize yourself with the specific requirements for your CMMC 2.0 level. This includes reviewing the relevant National Institute of Standards and Technology (NIST) SP 800-171 and SP 800-172 controls and ensuring your systems align with these standards.
- **Conduct Internal Assessments:** Perform thorough internal assessments to identify any vulnerabilities or gaps in your current cybersecurity practices. Address these issues before undergoing an official assessment.
- **Develop a Compliance Plan:** Create a detailed plan that outlines the steps needed to achieve compliance. This should include timelines, responsible parties and specific actions to be taken.
- **Engage with Third-Party Assessors:** Schedule and prepare for a third-party assessment by a CMMC Third Party Assessment Organization (C3PAO) to conform to higher levels of CMMC 2.0 compliance. Ensure you understand the process and requirements for these assessments.
- **Continuous Monitoring and Improvement:** Implement continuous monitoring and logging of system activities. Regularly review and update your cybersecurity practices to address new threats and maintain compliance.
- **Utilize Available Resources:** Take advantage of resources provided by the CMMC Accreditation Body (CMMC AB), including training programs, guidance documents and other support materials to better understand the certification process.
- **Document Everything:** Maintain thorough documentation of all cybersecurity policies, procedures and practices. This documentation will be crucial during the assessment process.

By following these steps, contractors can better prepare for CMMC 2.0 assessments and ensure they meet the necessary compliance standards.

How CrowdStrike Supports CMMC 2.0 Compliance and Cyber Resilience

CrowdStrike's solutions provide the following benefits to DIB partners:

Iterative Process for Higher Levels: As contractors progress through different CMMC 2.0 levels, CrowdStrike supports an iterative process of enhancing security measures. This includes managing devices, ensuring only authorized access to network resources and integrating mobility management components.

Comprehensive Security Management: CrowdStrike offers a full suite of tools for managing incident response, risk, authentication and access control, aligned with DoD-defined NIST controls.

Speed and Efficiency: CrowdStrike's solutions can help contractors achieve compliance quickly, potentially over a weekend, due to the efficiency, scalability and flexibility of the CrowdStrike Falcon® cloud-native software-as-a-service (SaaS) platform.

Ease of Deployment: CrowdStrike's solutions are designed for rapid and straightforward deployment, minimizing downtime while integrating with existing investments to bolster cybersecurity.

Administration: The Falcon platform offers user-friendly administration features, making it easier for organizations to manage their cybersecurity posture.

This structured approach highlights CrowdStrike's strengths and how they support DIB contractors in achieving and maintaining CMMC 2.0 compliance.

Navigating the Complexities of CMMC 2.0 Compliance

CrowdStrike stands ready to support DIB contractors in navigating the complexities of CMMC 2.0 compliance. Utilizing our comprehensive suite of security solutions, we offer robust protection, efficient deployment and continuous monitoring to ensure that contractors not only meet but exceed the required standards. By partnering with CrowdStrike, DIB contractors can confidently address the challenges of compliance, secure their systems against advanced threats, and contribute to the overall resilience of the U.S. defense infrastructure.

As the July 2025 compliance deadline approaches, it is imperative for all DIB partners to invest in their cybersecurity capabilities. Through thorough preparation, strategic planning and leveraging the expertise of trusted partners like CrowdStrike, contractors can achieve and maintain the highest levels of cybersecurity, ensuring the protection of sensitive information and the continued success of their missions.

Partner with CrowdStrike today to assess your current security posture, identify any gaps and create a comprehensive plan that ensures all CMMC 2.0 requirements are fully met before the deadline.

CrowdStrike's Alignment with CMMC Compliance Requirements

CrowdStrike's suite of technologies maps directly to the controls required for CMMC compliance across Levels 1, 2 and 3. Each solution — such as Falcon Insight XDR, Falcon Identity Protection and Falcon Exposure Management — meets or supports specific cybersecurity domains outlined by CMMC, including access control, risk assessment and incident response. These visual representations serve as a practical guide for DIB contractors, showcasing how CrowdStrike's offerings comprehensively address the rigorous standards of the CMMC framework. By leveraging these technologies, contractors can confidently align their security postures with compliance requirements, ensuring readiness for certification while strengthening their defense against evolving threats.

LEVEL 1

Legend: Meets / Supports		Cybersecurity Maturity Model Certification (CMMC) 2.0 Alignment						
		Access Control	Identification and Authentication	Media Protection	Physical Protection	System and Communication Protection	System and Information Integrity	
Level 1	Falcon Platform	Falcon Insight XDR	✓	✓			✓	✓
		Falcon Prevent (NGAV)						✓
		Falcon Discover		✓				
		Falcon Device Control	✓					
		Falcon Firewall Management	✓					
		Falcon Data Protection	✓				✓	
		Falcon Identity Protection	✓	✓			✓	
		Falcon Next-Gen SIEM					✓	✓
		Falcon Fusion						✓

LEVEL 2

Legend: Meets / Supports		Cybersecurity Maturity Model Certification (CMMC) 2.0 Alignment													
		Access Control	Awareness and Training	Audit and Accountability	Configuration Management	Identification and Authentication	Incident Response	Maintenance	Media Protection	Personnel Security	Physical Protection	Risk Assessment	Security Assessment	System and Communication Protection	System and Information Integrity
Level 2	Falcon Platform	Falcon Insight XDR	✓		✓	✓	✓	✓	✓			✓	✓	✓	✓
		Falcon Prevent (NGAV)	✓			✓		✓				✓	✓		✓
		Falcon Discover	✓			✓	✓						✓		
		Falcon Identity Protection	✓		✓		✓	✓				✓	✓	✓	✓
		Falcon Device Control	✓		✓				✓					✓	
		Falcon Data Protection	✓						✓					✓	
		Falcon Firewall Management	✓											✓	
		Falcon FileVantage			✓	✓									
		Falcon for Mobile	✓											✓	
		Falcon Adversary Intelligence		✓											
		Exposure Management (Spotlight)										✓	✓		
		Falcon for IT (FIT)				✓						✓			
		Falcon Cloud Security (FCS)				✓						✓			
		Falcon Fusion (SOAR)													✓
		Falcon Next-Gen SIEM			✓		✓						✓	✓	✓

LEVEL 3

Legend: Meets / Supports		Cybersecurity Maturity Model Certification (CMMC) 2.0 Alignment										
		Access Control	Awareness and Training	Audit and Accountability	Configuration Management	Identification and Authentication	Incident Response	Personnel Security	Risk Assessment	Security Assessment	System and Communication Protection	System and Information Integrity
Level 3	Falcon Platform	Falcon Insight XDR	✓		✓		✓	✓			✓	✓
		Falcon Prevent (NGAV)			✓		✓					✓
		Falcon Identity Protection	✓			✓	✓	✓			✓	✓
		Falcon Firewall Management	✓									
		Falcon Discover			✓							
		Falcon Exposure Management (Spotlight)					✓		✓	✓		
		Falcon for IT (FIT)			✓							
		Falcon Data Protection							✓		✓	
		Falcon Cloud Security (FCS)			✓		✓		✓			
		Falcon Discover for IoT										✓
		Falcon Insight for IoT										✓
		Falcon FileVantage			✓							✓
		Falcon Next-Gen SIEM					✓					✓
		Professional Services					✓					
		Falcon Adversary OverWatch					✓		✓			✓
		Falcon Complete					✓					
		Falcon Adversary Intelligence					✓		✓			✓

About CrowdStrike

[CrowdStrike](#) (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world’s most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: <https://www.crowdstrike.com/>

Follow us: [Blog](#) | [X](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>