Everforth
ECS Federal

Cybersecurity Maturity Model Certification 2.0

As Cybersecurity Maturity Model Certification (CMMC) requirements continue to be incorporated into Department of War (DoW) contracts, organizations across the Defense Industrial Base (DIB) face increasing pressure to demonstrate that they can adequately protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Achieving CMMC compliance requires more than satisfying technical security controls—it requires a strategic approach to governance, documentation, risk management, and operational maturity. Organizations that proactively prepare for CMMC will not only improve their cybersecurity posture but also strengthen their ability to compete for and retain valuable defense contracts. **As the DoW continues its phased implementation of the CMMC Program, organizations that delay preparation may face increased compliance challenges and reduced eligibility for future defense opportunities.**

CMMC 2.0 at a glance

Three
maturity levels

110+
cybersecurity best practices

Assessments
All companies in the DIB must complete a CMMC assessment

What is CMMC?

The foundation of CMMC is based on NIST SP 800-171 and other key cybersecurity best practices.

LEVEL 1 is foundational and has 17 practices to follow. It requires self-assessment and is intended for companies that handle Federal Contract Information (FCI) only.

LEVEL 2 is more advanced and is intended for companies that also handle Controlled Unclassified Information (CUI). It consists of 110 practices.

LEVEL 3 is expert and includes the 110 practices plus 24 enhanced security requirements. It is more rigorous and requires formal government assessments.

Solutions/Technology Areas by CMMC level

LEVEL 1

- NGAV
- EDR
- Application Management
- Account Monitoring
- Media Sanitization

LEVEL 2

- SIEM
- Vulnerability Management
- Removable Media Device Control
- Privileged Account Management
- Backups
- Encryption
- SOAR
- Threat Intelligence Platform
- Mobile Device Security
- Security Awareness Training
- Multi-Factor Authentication (IA.L2-3.5.3)
- Data Classification
- Data Loss Prevention
- Wireless Access Point Security (AC.L2-3.1.17)
- Firewall (SC.L2-3.13.6)
- Zero-Trust Network Access (SC.L2-3.13.7)
- CASB
- Email Security

Additional Cybersecurity Best Practices

- NAC
- Security Awareness – Additional Focused Areas
- Threat Intelligence Data Feeds
- Threat Intelligence Platform
- Penetration Testing
- Third-Party Cyber Risk Management
- Web Gateway
- Sandboxing
- Systems Component Discovery and Inventory (e.g., firmware level, OS type)
- Deception
- Application Whitelisting (CM.L2-3.4.8)
- Security Operations Center
- Rogue Network Device Identification
- Data Integrity
- Digital Forensics
- Cyber Incident Response Team
- Packet Collection & Storage
- UEBA

The Everforth ECS Solution

Everforth ECS has more than 20 years' experience providing risk mitigation and compliance services to companies who do business with the federal government – and the expertise to help companies of all sizes achieve CMMC compliance. We've built strong, long-lasting relationships with some of the world's leading public agencies and private companies.

Our cybersecurity experts will do more than simply help you pass an assessment – we will work closely with your team to improve your cybersecurity posture, with managed service offerings ranging from SIEM and EDR to account monitoring and data loss prevention.

Ready to forge your path to CMMC compliance and ensure your continued success?
Reach out today at cyber@EverforthECS.com

V071326