REDSEAL

STAY AHEAD WITH REDSEAL

Navigating DoD's Cybersecurity Maturity Model Certification

The Cybersecurity Maturity Model Certification (CMMC) remains pivotal for defense contractors and entities handling Controlled Unclassified Information (CUI). A third-party assessment across five levels ensures enterprises security maturity, which is vital for safeguarding national interests. CMMC builds upon NIST SP 800-171 compliance, with 110 security controls established by SP 800-171 extending its scope and rigor.

The foundation of the 171 practices across 17 security domains is necessary to reach the highest level of CMMC. Each Request for Proposal (RFP) will state the level of certification required to be awarded the contract.

The Department of Defense (DoD) is progressing towards integrating CMMC into contracts, aiming for full implementation by 2025. The CMMC Accreditation Body oversees Third-Party Assessment Organizations (3PAOs) responsible for auditing. Certification is expected to be valid for three years and ongoing compliance with the specified level is necessary.

For more information, visit **U.S. Department of Defense**.

Staying ahead with RedSeal

RedSeal's military grade network exposure management platform helps automate or partially automate many of the controls required by CMMC. Many of these controls are tedious to complete and must be checked repeatedly at specific intervals determined by NIST 800-171. By continuously monitoring controls, RedSeal streamlines preparation for recertification audits, eliminating the need for your team to review tens of thousands of lines of firewall rules while sifting through hundreds of spreadsheets to access control lists and ensure compliance.

Through comprehensive and continuous inspection, RedSeal provides a risk-based audit of a network and continuously monitors its security posture. Operators and leadership can track trends in defensive operations over time using RedSeal's Digital Resilience Score, which also measures vulnerability management, secure configuration management, and network understanding.

RedSeal's platform visually represents what is on your network, how it's connected, and the associated risk. With RedSeal, you can visualize end-to-end access, both intended and unintended, between any two points of the network, accelerating incident response.

This visualization includes detailed access and attack paths for individual devices in the context of exploitable vulnerabilities, aiding decision-making during missions.

RedSeal builds a complete model of your network—including cloud, SDN and physical environments—using configuration files retrieved dynamically or offline. It brings in vulnerability and all available endpoint information, enabling your teams to validate that network segmentation is in place and configured as intended.

RedSeal checks all devices for compliance with industry best practices and standards such as DISA STIGs and NIST guidelines. This proactive automation significantly reduces audit preparation time (including CCRI and others) and assists with speedy remediation.

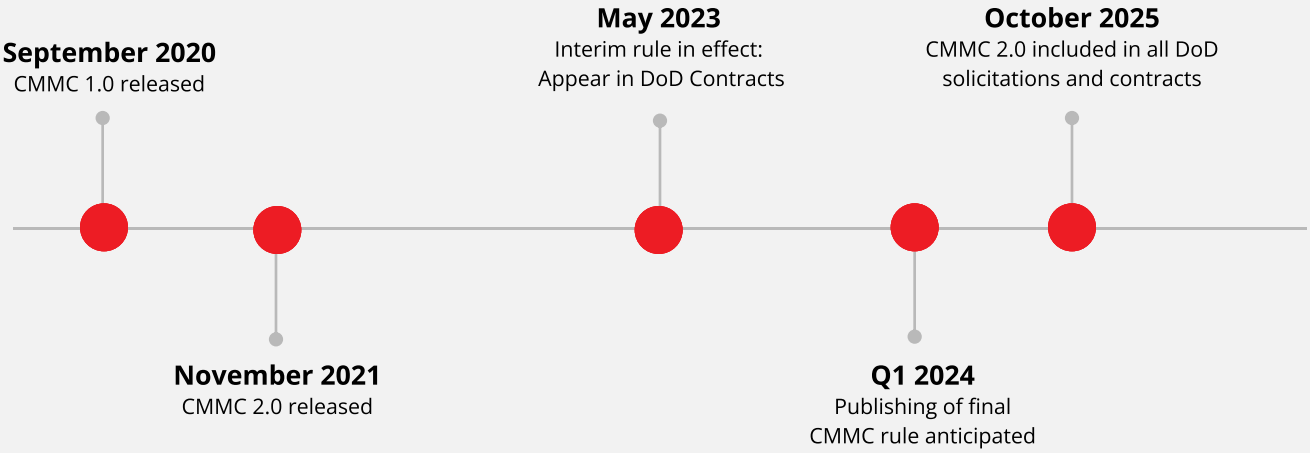
Achieving CMMC basics

RedSeal can support organizations through each level of CMMC 2.0. Below is an outline of where organizations may fall within the Proposed Rule:

- **Level 3:** Highest level, for requirements with elevated security concerns, particularly to address the risk of an Advanced Persistent Threat.
- **Level 2:** One step below Level 3, will operate where most contractors burdened by DFARS 252.204-7012 have been required to operate.
- **Level 1:** A new requirement imposed upon contractors that may not have started their cybersecurity journey, will be assessed against an organization's ability to properly safeguard Federal Contract Information ("FCI").

As outlined by McCarter & English, specific CMMC Levels requirements can be found on **THIS** informational piece. RedSeal provides the DoD—as well as commercial, civilian, intelligence organizations—with real-time understanding and a model of their cyber terrain so they can discover, detect, analyze and mitigate threats and deliver resilience to the mission.

CMMC 2.0 Phased Implementation



Sourced from CIMCOR "Top 10 Things to Know About CMMC