CMMC AND REDSEAL

Be Prepared with RedSeal: DOD-Required Cybersecurity Maturity Model Certification

Cybersecurity Maturity Model Certification (CMMC) is a tiered system in which defense contractors—or any organization with Controlled Unclassified Information (CUI) must be vetted by a third-party assessor on a five-level scale to determine the maturity of their enterprise security. Simply stated, this requires companies that do business with the Department of Defense to protect their data since it is critical to national security and America's competitive military edge. CMMC is an expanded and enhanced version of NIST SP 800-171 compliance. The 110 security controls established by SP 800-171 are the foundation of the 171 practices across 17 security domains required to reach the highest level of CMMC. Each Request for Proposal (RFP) will state the level of certification required to be awarded the contract. It is expected for CMMC Level 3 certification to be the de facto standard for most organizations to do business with the DOD—with Levels 4 and 5 reserved for more sensitive projects. The DOD is working on a DFARS rule change to incorporate CMMC into contracts by Fall 2020, although full roll-out is targeted for 2025.

A non-profit organization, the CMMC Accreditation Body has been established to oversee certification of Third-Party Assessment Organizations (3PAOs), assessors who will serve as auditors. A certification is expected to be valid for three years.

CMMC is an expanded and enhanced version of NIST SP 800-171 compliance. The key differences are:

- Enhanced controls for Levels 4 and 5
- Requirement for third-party audit instead of self-certification

How Can RedSeal Help?

RedSeal's military grade cyber terrain analytics platform helps automate 67 of the 171 controls in CMMC. Many of the controls are tedious to complete and must be checked repeatedly at specific intervals determined by NIST 800-171. By using RedSeal, your team can quickly identify where your network has drifted out of compliance, allowing them to rapidly remediate identified misconfigurations without having to pore over hundreds of spreadsheets, reviewing tens of thousands of lines of firewall rules and access control lists to determine if you are still compliant.

Additionally, when it comes time for re-certification you can rest assured that your company is prepared for the audit, because RedSeal has been continuously monitoring the configuration state of those 67 controls, allowing your network and cybersecurity teams to efficiently use their time keeping the business prepared and mission ready.

REDSEAL

1600 Technology Drive, 4th Floor, San Jose, CA 95110

+1 408 641 2200 | 888 845 8169 | redseal.net | info@redseal.net

CMMC AND REDSEAL

This comprehensive, continuous inspection allows RedSeal to report a risk-based audit of a network and then continuously monitor its security posture. Operators and leadership can track how defensive operations are trending over time via RedSeal's Digital Resilience Score, which also measures vulnerability management, secure configuration management, and understanding of the network.

RedSeal's platform shows you what is on your network, how it's connected and the associated risk. With RedSeal, you can visualize end-to-end access, intended and unintended, between any two points of the network to accelerate incident response. This visualization includes detailed access and attack paths for individual devices in the context of exploitable vulnerabilities to speed decision making during a mission.

RedSeal builds a complete model of your network—including cloud, SDN and physical environments—using configuration files retrieved either dynamically or completely offline. It brings in vulnerability and all available endpoint information. Your teams will be able to validate that network segmentation is in place and configured as intended. RedSeal checks all devices to see if they comply with industry best practices and standards such as DISA STIGs and NIST guidelines. This proactive automation greatly reduces audit prep time (CCRI, others) and assists with speedy remediation.

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.

RedSeal helps automate 67 CMCC controls across 5 levels

Level 1 – 5 of 17

Level 2 – 31 of 72

Level 3 - 48 of 130

Level 4 – 60 of 156

Level 5 – 67 of 171

BATTLE TESTED

RedSeal Department of Defense Clients

To schedule a demo, or for more information, go to https://www.redseal.net/government/dod/.

CMMC TIMELINE			
Late 2019	**Jan 2020**	**Summer 2020**	**Fall 2020**
DOD releases draft CMMC levels and associated NIST controls for feedback Announces non-profit in charge of certifyng third-party auditor	CMMC Levels and requirements released Program to certify auditors underway	CMMC requirements appear in DOD RFIs Third party auditors begin CMMC certification assessments	DOD contractors must be certified to bid on RFPs as early as September

REDSEAL

1600 Technology Drive, 4th Floor, San Jose, CA 95110

+1 408 641 2200 | 888 845 8169 | redseal.net | info@redseal.net