



CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) AND NETWORK DEFENDER®

The CMMC program is a driving factor in the cybersecurity strategy of just about any organization that does business with the Department of Defense. Celerium’s Network Defender solution can help companies comply with CMMC requirements.

Network Defender supports 12 out of 110 (11%) of 800-171 Controls OR CMMC 2.0 Practices. Moreover, in terms of the SPRS (Supplier Performance Risk System) scoring for 800-171, the solution supports 42 of the 110 points (38% of total SPRS points) since many of the supported controls are weighted 5 points. The table below lists the CMMC controls supported by the Network Defender platform.



Domain	800-171 Security Controls	CMMC 2.0 Practice	Description	SPRS Scoring Points
Access Control	3.1.12	AC.L2-3.1.12	Control Remote Access	5
Audit	3.3.1	AC.L2-3.3.1	System Auditing	5
	3.3.3	AC.L2-3.3.3	Event Review	1
	3.3.5	AC.L2-3.3.5	Audit Correlation	5
	3.3.6	AC.L2-3.3.6	Audit Reduction & Reporting	1
	3.3.8	AC.L2-3.3.8	Audit Protection	1
	3.3.9	AC.L2-3.3.9	Audit Management	1
	Incident Response	3.6.1	IR.L2-3.6.1	Incident Handling
3.6.2		IR.L2-3.6.2	Incident Reporting	5
3.6.3		IR.L2-3.6.3	Incident Response Testing	1
System & Communications Protection	3.13.1	SC.L2-3.13.1	Boundary Protection	5
	3.13.6	SC.L2-3.13.6	Net Comms by Exception	5
System & Information Integrity	3.14.3	SC.L2-3.14.3	Security Alerts & Adversaries	5
	3.14.6	SC.L2-3.14.6	Monitor Comms for Attacks	5
	3.14.7	SC.L2-3.14.7	Identify Unauthorized Use	3
Total SPRS 800- 171/ CMMC 2.0	15 Controls	5 Domains		53 Points