The United States' Department of Defense (DoD) supply chain is one of the most critical to both national security as well as the protection of the individuals in the armed forces. Regardless of where contractors sit in that supply chain, security is crucial to avoid intellectual property theft or worse, sabotage from cyber criminals and nation-states engaged in cyber warfare.

The Cybersecurity Maturity Model Certification (CMMC) has been developed in partnership with academia (Johns Hopkins and Carnegie Mellon) and industry leaders in the form of a listening tour and draws from a library of standards and frameworks, including NIST SP 800-171 and the NIST Cybersecurity Framework.

Accelerating the DFARS to CMMC Transition

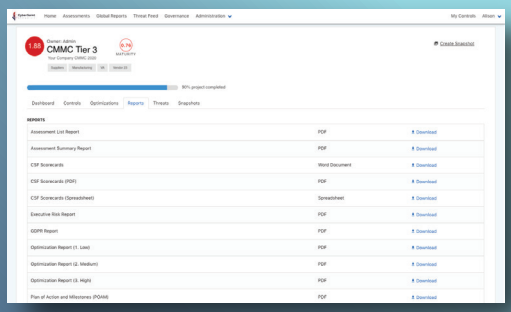
Post-DFARS (NIST SP 800-171) and upon developing the CMMC, the DoD recognized that not all contractors have the bandwidth to develop security programs on par with a prime nor should they have to. Recognizing that contractors' security should be dependent on the form and caliber of controlled unclassified information (CUI) that they are working with, the CMMC is a tiered model. Ranging from Tier 1 (Basic Cyber Hygiene) to Tier 5 (Advanced/Progressive), the levels are designed to enable vendors to meet the requirements necessary for the contract they are bidding for rather than having to invest in unnecessary requirements meant for a higher bid.

The CMMC is composed of Domains that are in turn broken down into respective processes and practices that support a given Domain. The integration of both practices and processes to support the desired Tier certification is new and brings about new challenges for contractors looking to achieve that certification using spreadsheets.

Because the CMMC Tier structure is cascading, to achieve a Tier Three certification, a contractor must meet the requirements of Tiers One, Two, and Three. If a contractor does not have a process required to meet Tier Two, they will not be certified for Tier Three. Where contractors had the potential to achieve DFARS compliance using spreadsheets given the checklist format, the CMMC workflow calls for a more advanced solution to achieve and maintain a Tier certification. CyberStrong automates organizations' transition from in-progress initiatives or DFARS compliance achievement to CMMC success.

Get Going on the CMMC in Hours and Scale Cyber Maturity Over Time

For organizations who want to stand up a program around cybersecurity maturity that is agile, customized, and scalable, CyberStrong allows information security teams to quickly baseline their programs and suppliers alike on the Cybersecurity Maturity Model Certification, prioritize where to remediate based on high Return on Security Investment, and have confidence in their practices and processes at time of award.



info@cybersaint.io | (877) 647-8273

How CyberStrong Supports CMMC Programs

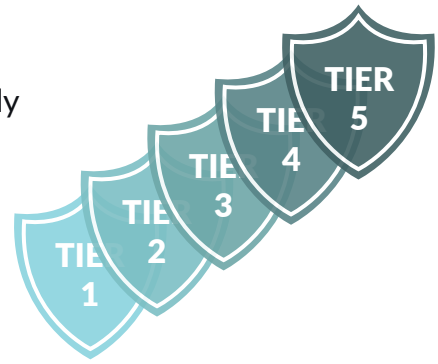
Analyze what practices you're doing and how well your process performs on the CMMC

The scoring of Processes and Practices within CyberStrong are discerned together - helping to both contextualize maturity as well as help you and your team know tactical requirements that you've completed or have yet to complete.

Know Where You Stand on CMMC Tiers 1-5

Automated Tier Scoring Logic - The CyberStrong platform automatically indicates at what Tier your current processes and practices are. As you move through the assessment, the backend logic will update in real-time, indicating what at what Tier you currently stand.

Clearly understand where you and your organization stand on the CMMC with automated Tier scoring based on assessment responses.

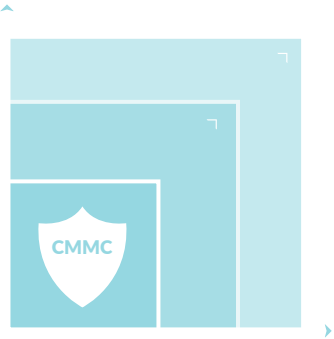


Justify CMMC Compliance at Time of Award with Confidence

With a real-time reporting engine designed for CMMC auditors and ready for automatic download, you can deliver the most up to date cybersecurity program data without any of the menial aggregation efforts that teams experience when assessing with spreadsheets.

Scale Your CMMC Compliance with CyberStrong

CyberStrong is designed to scale with your program maturity. Because the information is fully integrated and centralized, as your program improves and you seek higher Tier certification on the CMMC, CyberStrong enables you to win more business faster.

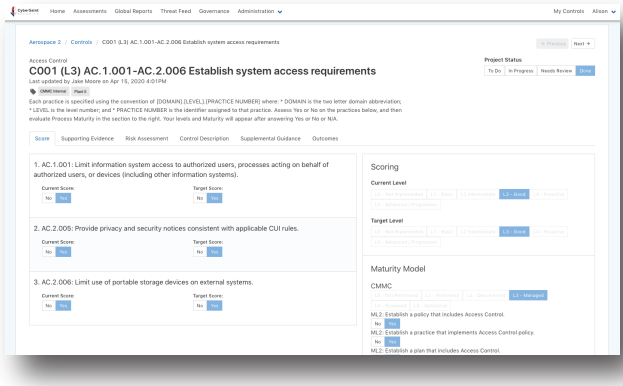


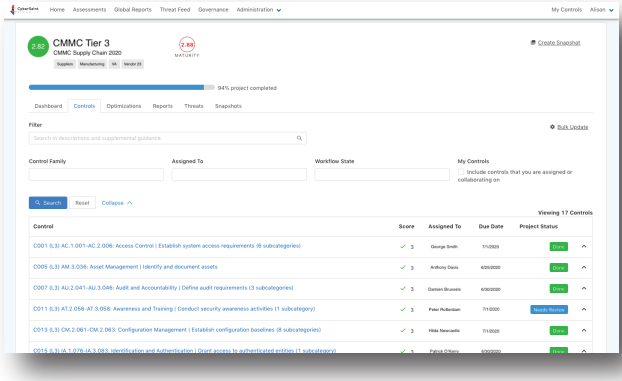
info@cybersaint.io | (877) 647-8273

Streamline Strategy, Process, and Reporting

Define Clear Roles and Access for Assessors and Audit

Built to enable all stakeholders in the organization, CyberStrong allows managers and collaborators to conduct assessments and an Observer role for CMMC auditors. Because the information is all in one place, your C3PAO will be able to get the most up to date information within a fraction of time.





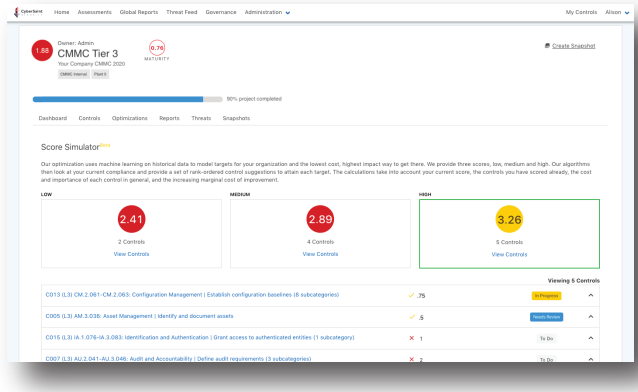
Centralize Internal Risk and Compliance with Supply Chain Risk Management

The fully integrated capabilities of CyberStrong enable you to assess both internal risk and compliance and that of your supply chain in parallel. Using CyberStrong's Governance Dashboards, you can see how your vendors compare against each other and where the weak points are in your supply chain.

For contractors a commitment to ensuring that suppliers are CMMC compliant is paramount. Managing your supply chain out of CyberStrong drastically reduces the effort needed to help your vendors achieve compliance with enhanced results.

Leverage AI Backed Remediation Paths and Generate Measurable RoSI

Following a baseline assessment, teams often are stuck trying to figure out where to start to achieve compliance. CyberStrong's AI-backed remediation paths deliver clear paths to compliance and points your team towards controls with the lowest-cost and highest-ROI for your program.



info@cybersaint.io | (877) 647-8273