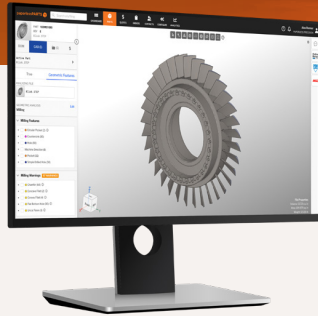


Be the Shop Defense Contractors Can Trust

What every job shop needs to know about getting ready for CMMC.



Paperless Parts: A Secure Solution for Your Shop

Paperless Parts' is designed to specifically support the proper handling of CUI and support our customers' efforts towards CMMC compliance. Specifically, we:

- Adopt FedRAMP Moderate as the baseline for our Security System Plan
- Retain top two FedRAMP-recognized 3PAOs for advisory and assessment
- Hire only US Persons for roles requiring privileged access.
- Maintain our ITAR registration
- Host all infrastructure on AWS GovCloud (the same servers used the by DoD) and use other FedRAMP services
- Define and document a shared responsibility model (Customer Responsibility Matrix).
- Continue to invest in our security posture with a multi-million dollar budget dedicated to ensuring we maintain our compliance

In addition:

- All data is encrypted in-transit using TLS v1.2 with modern ciphers
- Uploaded files are encrypted at rest with AES-256 encryption
- Network and servers are approved for CUI
- Customers' files are never sold or shared with third parties
- All data is securely backed up nightly
- Customers always retain ownership on all data you upload
- Access to the platform is controlled through Identity Provider support for Single Sign-On
- Only users with rights to certain features are available through intelligent user permissions for viewing, sharing, modifying, and downloading sensitive information
- Audit reports of who has viewed or interacted with sensitive data are available as needed

Over the next few years, every business in the defense manufacturing supply chain—an estimated 300,000 companies—will need to obtain third-party certification in cybersecurity. The level of required security will depend on what kind of data is handled by each company. Are you prepared?

Cybersecurity Maturity Model Certification (CMMC)

CMMC is a U.S. Department of Defense (DoD) program that applies to Defense Industrial Base (DIB) contractors. It is a unifying standard and new certification model to ensure that DoD contractors properly protect sensitive information. CMMC builds largely on the DFARS (Defense Federal Acquisition Regulation Supplement) and incorporates much of the pre-existing NIST (National Institute for Standard and Technology) 800-171 cybersecurity requirements. However, CMMC is different from previous cybersecurity standards in that self-reporting compliance is no longer enough. Rather, certification by third-party auditors will be a precondition for quoting work. **This is a major game changer for job shops.**

What You Need to Know Now

CMMC is expected to be required in DoD contracts starting in early 2025, but CMMC requirements are already being incorporated into RFQs – which means if you don't already have a plan in place, now is the time to start getting prepared. CMMC requirements will be introduced gradually to more contracts over time, and but if you wait until required by a contract to think about cybersecurity compliance, it will be too late. It's estimated that CMMC certification can take 1-2 years from start to finish. It takes a typical shop many months to assess their processes and remediate security gaps.

(Think of it as roughly similar to the process of getting ISO 9001/AS9100 certified). And third-party certification takes additional time. Shops that are ahead of the game have an opportunity to differentiate themselves with buyers.

Certification by third-party auditors **will be a precondition for quoting work.**

What Every Job Shop Needs to Know About Getting Ready for CMMC



Seven Steps to Get Ready for CMMC

1 Identify Which CMMC Tier Is Right for

There are three tiers of CMMC Certification. Level 1 is considered foundational. Level 2 is considered “Advanced.” Any shop working with CUI will need this level of compliance, which requires the implementation of the 110 best security practices aligned with NIST SP 800-171. Level 3, or “Expert,” is the highest level of certification and requires an organization to follow a set of 110+ practices based on NIST SP 800-172.

2 Identify the Right Security Resources

Whether you have an in-house IT & Security team or need to outsource services, there’s a lot that goes into ensuring you have a solid security posture and you need to have a team you can trust.

3 Take a Pulse Check by Updating Supporting Documents

Create or update your System Security Plan. Identify where you have gaps and set a plan for addressing those in a Plan of Action & Milestones (POA&M).

4 Get Cracking on the “To Do” List

Use the items identified in the POA&M as a roadmap for work that needs to be completed ASAP.

5 Conduct a Self-Assessment

Confirm that your System Security Plan and all organizational standards, policies, and procedures are consistent.

6 Don't Stop There

Maintaining proper security posture isn’t a one-and-done exercise. Continuously maintain and refine your security program, invest in training, and keep documentation up to date.

7 Complete Your CMMC Audit

Once you are ready, identify a Cyber AB certified CMMC auditor to work with, and schedule your audit. There are a limited number of auditors available, so it is recommended to plan ahead so you don’t miss any important deadlines.

Frequently Asked Questions

Is Paperless Parts CMMC-Compliant?

Paperless Parts is designed for customers seeking CMMC Level 2 certification using us as a Cloud Service Provider. As required by ITAR, DFARS and CMMC requirements, we operate on US-based infrastructure, maintain 100% US Persons support staff, and have implemented the FedRAMP Moderate security controls which have been assessed and attested to by a FedRAMP-recognized third-party assessment organization.

Are CMMC compliance standards finalized?

Yes, requirements were finalized when the Department of Defense published the Final Rule in December 2023.

Why is CMMC important?

The U.S. projects its power via military technology, in which we’ve invested trillions of dollars over many decades. We have started to see adversaries field extremely similar systems at a fraction of the timeline and cost, most likely helped by the theft of intellectual property. As critical national infrastructure, manufacturing is a major target for cybercrime.

Businesses of all sizes and at any point in the supply chain are targeted. Cyberattacks cost businesses \$200,000 on average, and four in 10 companies have experienced multiple incidents. Research shows that the number of publicly recorded ransomware attacks against manufacturing has tripled in the last year alone—and even job shops and contract manufacturers are at risk: 43% of cyberattacks are aimed at small businesses. To protect CUI, the government needs to ensure that shops are taking appropriate steps.

Does every shop have to be audited and certified?

With CMMC 2.0, some companies with defense contracts will need third-party certification, while others will be able to self-assess. Every company with a defense contract is still required to implement NIST800-171, and must submit their Supplier Performance Risk System (SPRS) score.

Depending on the sensitivity of work performed, you may be asked to undergo a complete CMMC Audit. Even if your company is not pursuing Level 2 compliance, most shops do benefit from a third-party audit of their company’s cybersecurity architecture.

Who do I contact to conduct a CMMC Compliance audit?

Paperless Parts does not provide this service, however, we’re happy to work with you to provide recommendations as the landscape of services providers becomes clearer.

I don't make parts with CUI. Do I need to get CMMC certified?

No – but cybersecurity should be a top priority for all shops. More and more buyers are including cybersecurity in their vendor evaluation criteria. A buyer’s primary job is to manage risk. In addition to risks with hitting cost and delivery goals, part buyers are increasingly concerned about their intellectual property.

Where can I get additional, official information about CMMC?

<https://dodcio.defense.gov/CMMC/FAQ/>