paperlessPARTS

Want to Be the Shop Defense Contractors Can Trust?

CMMC requirements will begin hitting contracts in the early 2024 – 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 contracts, but if you wait until required by a contract to think about cybersecurity compliance, it will be too late. It takes a typical shop many months to assess and remediate gaps (think of it as roughly similar to the process of getting ISO 9001/AS9100 certified). Third-party certification takes additional time. **Shops that are ahead of the game have an opportunity to differentiate themselves with buyers. Are you prepared?**

5 Steps to Prepare for CMMC

Step 1: Identify which CMMC tier is right for your shop

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.

Step 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.

Step 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).

Step 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.

Step 5: Conduct a Self-Assessment

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

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.

Paperless Parts: A Secure Solution for Your Shop

- Hosted on Amazon GovCloud (the same servers used by the Department of Defense)
- ITAR-registered
- All data encrypted in-transit using TLS v1.2 with modern ciphers
- Always retain ownership on all data you upload
- Uploaded files are encrypted at rest with AES-256 encryption
- System Security Plan based on the FedRAMP Moderate baseline (NIST 800-53)
- All data is securely backed up nightly
- Network and servers approved for Controlled Unclassified Information
- Your files are never sold or shared with third parties
- 100% US-based system administrators and support team

Want to see how Paperless Parts can help you stay ahead of CMMC requirements?
Click here to schedule your free demo today.