CMMC 2.0 & Paperless Parts: What Job Shops and Contract Manufacturers Need to Know

paperlessPARTS

Contents

Introduction

Protecting your customers' data is one of your most important responsibilities. Whether you're making parts for the U.S. Department of Defense (DoD) and subject to the upcoming Cybersecurity Maturity Model Certification (CMMC) mandate, or making parts for other industries like medical devices, oil & gas, or agriculture/heavy machinery, your customers have invested heavily in research and development. It is your responsibility to make sure that intellectual property is treated appropriately.

This paper provides a brief background on CMMC and explains how Paperless Parts is helping to ensure that your data is secure.

Why CMMC and Why Now?

The Defense Industrial Base (DIB) spends billions of dollars annually to develop and build military technology: a development process that often takes years or decades. Foreign adversaries have become adept at attacking weaker points in the supply chain to shortcut that development process and produce cutting-edge technologies at a fraction of the price.

It is your responsibility to make sure that **intellectual property is treated appropriately.**

Why should job shops care? Simple: if you were a cyber criminal looking to steal controlled unclassified information (CUI), would you set your sights on a major defense contractor that spends millions of dollars on security and IT infrastructure, or would you try to seek out the most vulnerable, least secure parts of the supply chain?

Bottom line: you are the target.

The U.S. Government is clearly stepping up enforcement of ITAR (International Traffic in Arms Regulations) violations. In 2023, 3D Systems Corporation (3D) of Rock Hill, South Carolina, was slapped with a **$20M civil fine for ITAR violations**.

The goal of CMMC is to enhance the security and protection of CUI. These regulations apply to organizations of any size that handle, store, or access CUI, even those that believe they are exempt. The primary principles of the program are to:

- Safeguard sensitive information.
- Dynamically enhance the cybersecurity posture of the DIB.
- Ensure accountability while minimizing barriers to compliance with DoD requirements.
- Help instill a collaborative culture of cyber resilience and cybersecurity.
- Maintain and foster the public trust through high professional and ethical standards.

The best time to start implementing CMMC controls into your shop was two years ago; the second-best time is right now.

Manufacturers have long been the subject of standards and certifications around security, such as NIST (National Institute of Standards) 800-171. However, unlike those standards, which are self-reported, CMMC requires a third-party audit. Further strengthening the urgency around CMMC compliance, there are provisions in the Defense Federal Acquisition Regulation Supplement (DFARS), which both allow and mandate that the DoD require DIB contractors to attain and maintain a specified level of CMMC certification as a condition of contract award. Additionally, while DFARS compliance is self-reported, shops are always possible candidates for being audited by the Defense Contract Management Agency Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) to ensure they are meeting requirements of NIST 800-171. Some job shops are voluntarily signing up for these audits to prove their compliance and ensure that they are able to win defense jobs.

OUTCOMES OF WEAK SECURITY

Chinese copycats of U.S. military assets

In plain English: government contracts are only going to go to shops that are CMMC certified.

Creating even more headaches is the fact that there are a limited number of organizations that are qualified to administer CMMC audits, creating a significant backlog for those shops that are interested in pursuing CMMC certification.

Although costs and timeline to achieve CMMC compliance vary based on shop size and the type of CUI you're working with, most shops we work with at Paperless Parts are planning an implementation timeline of 1-2 years and budgeting for $100,000-$200,000 in costs.

In other words: if you want to continue to win these lucrative contracts, the best time to start implementing CMMC controls into your shop was two years ago; the second-best time is right now.

CMMC and Working with Cloud Service Providers

There are 110 controls called out in CMMC Level 2, and there is a tremendous amount of detail under each control. But surprisingly, there isn't a ton of specific guidance on how to evaluate cloud service providers (CSPs), such as Paperless Parts

Many shops are used to evaluating the cybersecurity of vendors in their supply chain, such as finishers, and shops have always asked about ITAR registration. Now, however, it's common to ask about progress toward CMMC. However, the requirements on cloud service providers are different and far more extensive than the requirements on manufacturers, so knowing what to ask is critical..

Under CMMC rules, the relevant details for how to assess CSPs comes from DFARS, which is a 2,000+ page document that outlines specifically how the DoD is allowed to spend money. In that behemoth of a document, the relevant clause to take note of is DFARS 7012, which states that if you're going to rely on a CSP to store CUI data, that service must have security controls in place equivalent to Federal Risk and Authorization Management (FedRAMP) Moderate baseline.

Unlike previous standards and regulatory compliance processes however, it's not simply a matter of taking your vendor's word for it. Under the CMMC Assessment Process (CAP), which is currently in draft form but not anticipated to meaningfully change, when shops get audited for CMMC compliance, your CSPs will have to provide a body of evidence that these security controls have been met.

Your CSPs will have to provide a body of evidence that **these security controls have been met**.

DFARS 7012

If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the **Contractor shall require and ensure that the cloud service provider meets** security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program **(FedRAMP) Moderate** baseline (https://www.fedramp.gov/resources/documents/) **and** that the cloud service provider **complies with requirements** in paragraphs (c) through (g) of this clause **for cyber incident reporting**, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

CMMC

December 2023: Proposed Final Rule

(ii) The Cloud Service Provider's (CSP) product or service offering is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline but meets security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline. Equivalency is met if the OSA has the CSP's System Security Plan (SSP) or other security documentation that describes the system environment, system responsibilities, the current status of the Moderate baseline controls required for the system, and a Customer Responsibility Matrix (CRM) that summarizes how each control is MET and which party is responsible for maintaining that control that maps to the NIST SP 800-171 Rev 2 requirements.

(iii) In accordance with [section sign] 170.19, the OSA's on-premesis infrastructure connecting to the CSP's product or service offerings is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the CRM must be documented or referred to in the OSA's System Security Plan (SSP).

How Paperless Parts Supports Your Path to CMMC Compliance

Paperless Parts has invested millions of dollars to ensure that your data is secure and protected. From our earliest days supporting ITAR-registered manufacturers to today supporting some of the most sophisticated government and defense contractors on the planet, we are committed to the continual investment in our platform to safeguard American intellectual property. The Paperless Parts for Aerospace and Defense solution is specifically tailored to ensure that we're constantly working with our customers to understand their unique security requirements and that we are the partner you can trust.

With over a million lines of code, listing out all of the security features and practices built into the platform would be too exhaustive to enumerate; however, we do think there are several key aspects of the platform—some newer than others—that are worth calling out:

We are committed to the continual investment in our platform **to safeguard American intellectual property.**

1. **Only U.S. Persons have access to CUI Data.** When you partner with Paperless Parts, we have a team of people—from our product and engineering team, to our onboarding and implementation team, to our customer success and support team—that are on call to help you succeed. As such, they sometimes require access to your Paperless Parts instance and data stored within the platform. Any Paperless Parts employee that has access to CUI data is a U.S. Person.

2. **Incident Reporting.** Of course, Paperless Parts has invested heavily to ensure that your data is always protected, but if we ever do have a security incident, Paperless Parts will follow the strict reporting guidelines outlined by the U.S. Government.

3. **FedRAMP Moderate Equivalence.** CSPs that are used by federal agencies are held to an even higher standard than CMMC, called the Federal Risk and Authorization Management Program (FedRAMP). While not directly used by the DIB, because Paperless Paperless works with hundreds of shops handling CUI, our platform has gone through a security assessment to demonstrate our commitment to implement robust security measures to protect sensitive data, and prove that we meet the requirements of FedRAMP. For context, CMMC has outlined 110 discreet controls for Level 2 compliance, whereas FedRAMP Moderate includes 325 controls outlined in a 500-page spec.

Other key characteristics of the Paperless Parts solution:

- Hosting on Amazon GovCloud, which is designed to allow U.S. government agencies (like the DoD) and their customers move sensitive workloads into the cloud.
- Network and servers approved for CUI. View and share controlled unclassified information securely within our system (and restrict who has access to it).
- Our platform is completely ITAR registered and compliant.
- All data in our system is securely backed up to 100% U.S.-based servers nightly.
- In-transit data encryption using TLS v1.2 with modern ciphers.
- Uploaded files encrypted at rest using AES-256 encryption.
- Retain full ownership over all data you upload to Paperless Parts.
- With intelligent permissions, designate which Paperless Parts users can view, download and/or share CUI.
- Flag files with CUI to enable viewing, downloading and sharing capabilities via intelligent permissions.
- Audit logs provide a record of who has interacted with CUI in the platform.
- Multi-factor authentication and Single Sign-On ensure system access only by authorized users.

The Shared Responsibility Model (and What it Means for Your Shop)

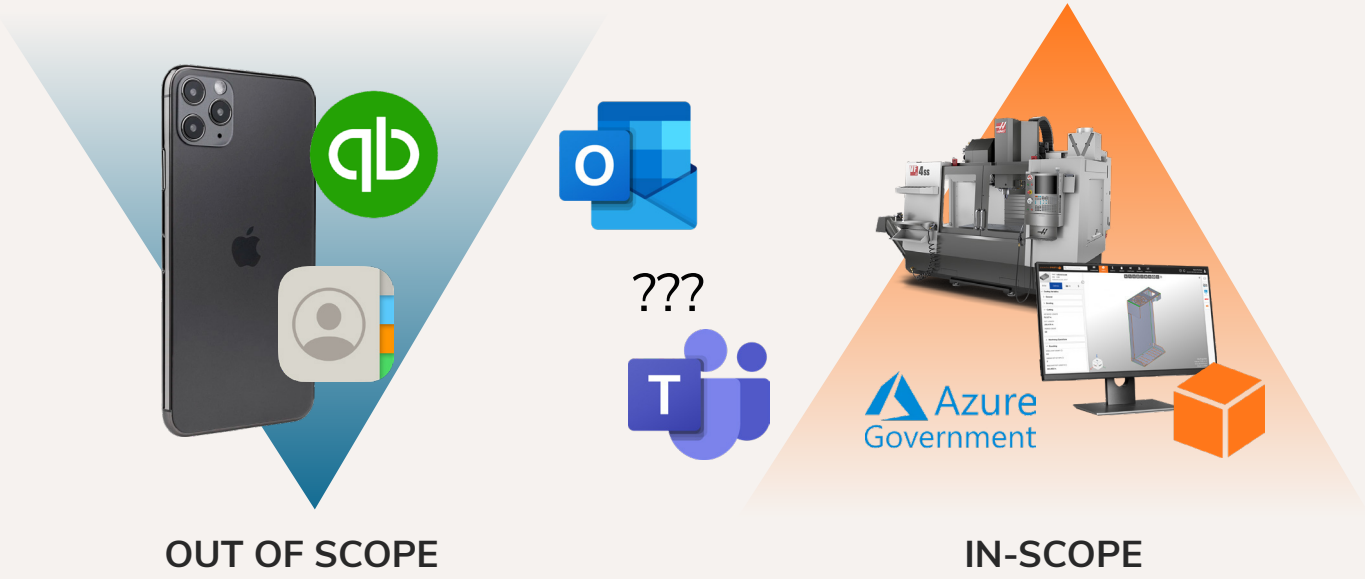
Successful implementation of CMMC controls requires that shops and CSPs work hand-in-hand to ensure data is safe and secure. While Paperless Parts has invested millions of dollars in the security of our platform and there are many controls that are 100% pre-configured by Paperless Parts, there are certain actions that are incumbent upon shop employees to ensure compliance, such as training your team on the proper handling of CUI, managing permissions based on your own Access Control Policy, and configuring workstations with session lock, banners/notifications, and Federal Information Processing Standard (FIPS)-mode enabling. We have worked to develop a detailed Customer Responsibility Matrix to ensure our customers are crystal clear about their responsibilities as it relates to configuring and maintaining Paperless Parts in a CMMC compliant manner.

One of the most critical responsibilities higlighted in our Customer Reponsibilitiy Matrix is that shops need to have selected and implemented their own Identity Provider and enabled it to manage Single Sign On (SSo) into Paperless Parts. SSO is the most straightforward way for your shop to meet all authentication-related CMMC requirements with Paperless Parts. This lets you set your password policy (including rules about password strength, expiration, re-use, etc), enforce multi-factor authentication, and remove access efficiently when needed such as when a user retires, all from one centralized system. With SSO, you configure your security preferences once, and it takes effect in all of your software tools, including Paperless Parts.

The goal for scoping CMMC boundaries should be **to keep the scope as small as possible—but no smaller.**

Where do you draw the line between what's in and out of scope for CMMC? Some systems, like Paperless Parts, are clearly in scope. Some systems, like your accounting software or customer relationship management (CRM) software, are very likely out of scope. But there are systems where individual shops will have to make a judgment call. Your email system, for example, could be in or out of scope. Shops need to ask themselves, "How are we going to be receiving files and tech packages with CUI? Are they coming through email or through a secure portal?"

What about collaboration tools like Microsoft Teams or Zoom? Are you sharing files or screen sharing CUI data? **Our advice: The goal for scoping CMMC boundaries should be to keep the scope as small as possible—but no smaller.**



How does CMMC apply to other third-party software besides Paperless Parts?

All network applications—on premise or in the cloud—that touch CUI data need to be properly secured in the manner defined by CMMC. The fastest and easiest way to do that is to only leverage third-party software, like Paperless Parts, that has done the work to build compliance into its offering.

However, if you use other third-party software solutions, there are alternate approaches. For example, you can build a layered security approach and require users to log in through a Virtual Private Network (VPN). The most important thing to do is to ask questions of your vendors: Are you FedRAMP Moderate equivalent? Is the infrastructure U.S.-based? Is your team staffed by U.S. persons? Do non-U.S. persons have remote access to my data?

Who makes the final call on CMMC boundaries?

With all these gray areas, making a call on where to set the boundaries can be tough. Ultimately, there is no cut-and-dried answer. Our best advice is to partner with a CMMC "Registered Practitioner" or "Registered Provider Organization." RP/RPOs are experts on the controls and process and are best qualified to guide you through the process (NOTE: Although we are always here to give you our best guidance, Paperless Parts is NOT, nor does it intend to be, a RP/RPO).

We also recommend talking to your defense customers. They should be able to help you think through what they consider CUI and what they don't. They should also be able to share with you how they plan to handle the transmission of CUI data: Are they going to continue to send it in email, or will they adopt a secure portal approach?

Conclusion

The implementation of Cybersecurity Maturity Model Certification (CMMC) has brought forth a multitude of questions and challenges in the realm of data security. Despite the extensive efforts and progress made over the past decade, the landscape we navigate is ever-evolving, with new threats and considerations arising on a daily basis.

In this era of uncharted territory, it is imperative for organizations to prioritize risk assessment and make informed decisions that bolster security measures and safeguard the intellectual property of their customers. While uncertainties persist, it is crucial to document these decisions within a System Security Plan and proceed confidently in our pursuit of enhanced data protection.

The journey towards CMMC compliance is ongoing, and it requires continuous vigilance, adaptability, and a proactive approach to address emerging security challenges. By embracing the CMMC framework and its associated practices, organizations can fortify their cybersecurity posture and contribute to the collective effort of safeguarding American intellectual property. Together, we can navigate this evolving landscape and uphold the security and integrity of our critical systems and data assets.

It is imperative for organizations to prioritize risk assessment and make informed decisions **that bolster security measures and safeguard the intellectual property of their customers.**