

CLIENT SUCCESS STORY

How Scientific Sales Maintains **Continuous CMMC Compliance**





Introduction

CMMC compliance is a heavy lift. That's why Jeff Barney engaged a trusted partner.



Client

Distributor of lab, safety, and industrial products that contracts with DoD



Challenge

Staff had no bandwidth to pursue CMMC compliance



Solution

CMMC compliance initiative + continuous monitoring and remediation



Results

Ready for the auditor (and equipped to stay compliant)

About Scientific Sales

Supplying critical equipment to the defense industry

[Scientific Sales](#) has developed long-term relationships with some of the highest quality manufacturers and suppliers in the laboratory, safety, environmental and industrial arenas.

The company also offers repair and rentals of environmental equipment. From laboratory supplies to respirators, law enforcement products, and more, Scientific Sales is a leading defense equipment distributor in many industries. The company is also a minority and woman-owned business, having served customers since 1987.



The Challenge

No bandwidth to pursue CMMC compliance

Scientific Sales is a small contractor out of Tennessee that does a lot of work for the federal government. The company needed to achieve [IT compliance](#) with the Cybersecurity Maturity Model Certification (CMMC) to handle projects from the Department of Defense.

While CMMC is a cybersecurity framework in the broadest sense, it doesn't focus heavily on the organization's overall cybersecurity posture. Rather, CMMC is intended to protect CUI (controlled unclassified information). There are many components to this, but risk management and continuous monitoring are two of the most critical.

As far as Scientific Sales knew, the company hadn't previously received any CUI—until they received three different pieces of CUI in six months.

Clearly, Scientific Sales needed to take action to comply with CMMC, ensuring they protected any CUI entrusted to them—both now and in the future.



CMMC in a nutshell

CMMC is a complex, lengthy regulation that uses NIST SP 800-171, revision 2, as its underlying framework. After several years of development, [CMMC has been finalized](#), going into effect December 16, 2024. The framework provides three levels of compliance:

- Level 1: 15 requirements for contractors who work with FCI (federal contract information).
- Level 2: 110 requirements for contractors who work with CUI (controlled unclassified information, as defined by the federal government).
- Level 3: roughly 140 requirements for contractors who work with CUI on highly sensitive projects; uses both NIST 800-171 and 172.

Resources needed to achieve CMMC compliance

Jeff Barney, eCommerce & IT Manager, knew that Scientific Sales would need to become Level 2 compliant. However, CMMC compliance is not a five-minute job. “It can take one person 40 hours a week for 18 months to complete the process,” Jeff said.

Clearly, achieving initial compliance is a heavy lift for an internal IT department—especially if your IT team is already working at capacity with day-to-day responsibilities.

But CMMC doesn’t stop with the first audit that you pass. Risk management evolves continuously, and that requires continuous monitoring and remediation.

As a smaller company, Scientific Sales didn’t have the available staff resources to achieve or maintain compliance. The company took the first step in compliance a few years ago, procuring a CMMC assessment from another provider. However, the assessment was very general—and it didn’t provide a path forward or comply with the new 2.0 standard.

The Solution

A smart, comprehensive approach to CMMC compliance

As a member of [Affiliated Distributors \(AD\)](#), Scientific Sales has access to a trusted network of providers to assist with all kinds of operational challenges. Here at Corsica Technologies, we are AD's preferred cybersecurity provider, and AD recommends our services to any member organization that needs assistance.

Once our teams were introduced to each other, the partnership was a natural fit, and Scientific Sales worked with us to do CMMC the right way. Our first order of business was to lock down CUI, so Scientific Sales could rest assured that this information was protected.

After achieving that, the company had breathing room to work on policies and procedures that required more time and effort. They also got the structure in place to handle risk management, continuous monitoring, and remediation. The Corsica plan covered:

- Access control
- Awareness and training
- Auditing and accountability
- Configuration management
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Personnel security
- Physical protection
- Risk assessment
- Security assessment
- System and communications protection
- System and information integrity

**A SMALL, MINORITY
AND WOMAN OWNED
BUSINESS**

Since 1987



Vicki Dyer, Owner & President



Under each of these items, Corsica and Scientific Sales dealt with numerous individual components that are required for compliance. The goal was to examine everything, determine where Scientific Sales was already compliant (and where they needed to invest some extra attention), and then create a roadmap for achieving and maintaining compliance.

Clearly, this was no small project. Jeff put it this way: "As you take steps and work with a good partner, CMMC is definitely doable. It just takes time and commitment to get it done."



"Picking a partner to assist in building those policies and procedures is huge."

Jeff Barney | E-Commerce & IT Manager
Scientific Sales

While Corsica guided the project, the working relationship was highly collaborative. "We were able to ask questions throughout the process for each control," Jeff said. "We were able to nail down exactly what we were missing."



The Results

CUI secured, roadmap defined, ready for the auditor

Scientific Sales is now ready for the CMMC auditor to go through all the high-level categories of compliance as well as the individual components of each category. In terms of risk management, Scientific Sales is in a great place. They can demonstrate to the auditor that they're taking proactive measures to understand and mitigate the risks that they face in handling CUI.

“We’ve got policies and procedures that we can work with now and customize to our liking.”

Jeff Barney | E-Commerce & IT Manager | Scientific Sales

Of course, you can't control what you can't see. That's why continuous monitoring is such a crucial piece of CMMC compliance.

Scientific Sales now has the processes and resources in place to perform continuous monitoring. The company is collaborating closely with Corsica Technologies, and the combined team has comprehensive visibility into everything that's happening in the company's environment. Corsica and Scientific Sales are maintaining compliance through regular initiatives, such as:

- Risk assessments
- Vulnerability scanning
- [Penetration testing](#)
- Employee awareness training

That last point is critical. Think about it from the attacker's standpoint. Why spend a week or a month trying to hack into your systems—when they can trick your employees into giving away their passwords? This is why [phishing email testing](#) is a cornerstone of the cybersecurity awareness training that Scientific Sales receives from us.



The Future

Continuous CMMC compliance

It's rare for an organization's technology infrastructure to remain static for long periods of time. Most companies continue to add new systems and decommission old ones. This involves making changes to business processes—including how you store, process, and transmit data like CUI. It's essential to stay on top of this and maintain CMMC compliance continuously.

Jeff and the team understand this challenge. "You're going to grow," Jeff said. "The company's going to change. Whatever adjustments you need to stay compliant, even after you become compliant, is going to be a huge deal."

"Having those tools and those relationships in place to help you continue the process, even after becoming compliant, is huge."

Jeff Barney | E-Commerce & IT Manager | Scientific Sales





ABOUT CORSICA TECHNOLOGIES

Corsica Technologies is a strategic technology partner specializing in consulting and managed services. With an integrated team of experts in cybersecurity, IT services, AI solutions, digital transformation, EDI, and data integration, Corsica offers comprehensive coverage and unlimited service consumption for one predictable monthly price—whether fully managed or co-managed.

YOUR TRUE TECHNOLOGY PARTNERSHIP STARTS HERE

Schedule a free consultation with our specialists to learn how technology can enable and transform your business.

 corsicatech.com

 [\(855\) 411-3387](tel:(855)411-3387)

Mid-Atlantic

508 Rhett Street
Greenville, SC 29601

Midwest

9921 Dupont Circle Dr West
Ft. Wayne, IN 46825

Southeast

1721 Goodrich Street
Augusta, GA 30904