Summary

A major DoD aerospace engineering partner for manufacturers in the Defense Industrial Base (DIB), was concerned about their lack of a compliance program. Knowing CMMC was advancing in rulemaking stages, it would be a matter of time before contract requirements included CMMC certification. Working with SP6 CRC's team of CMMC consultants, the organization was able to build a sustainable compliance program.

Key Takeaways from the Engagement:

- ✓ **Early scoping and realistic planning** are critical for building a CMMC program from scratch.
- ✓ **Integrating security into business processes** ensures long-term sustainability.
- ✓ A competent consulting team bridges the gap between IT operations and regulatory compliance.
- ✓ Documentation and training are just as important as technology controls.
- ✓ **CMMC preparation is a strategic investment**, not just a checkbox exercise.

CASE STUDY

AEROSPACE MANUFACTURER BUILDS A RESILIENT COMPLIANCE PROGRAM

SP6 Cyber Risk & Compliance

The Problem

This organization was aware their environment contained CUI, but was unaware of where the CUI was located, how to control it, and the overall security compliance status of their organization. The firm had basic IT and cybersecurity practices in place, but no formalized compliance program aligned with NIST SP 800-171 or the CMMC framework.

Recognizing the complexity and scale of the task, this DIB partner engaged with SP6 CRC's team of Certified CMMC Professionals for personalized consulting that would bolster a functioning compliance program to carry them to, and pass, a CMMC C3PAO assessment.

Solution

Our team of Certified CMMC Assessors began by conducting a security gap assessment to identify where the organization's current security practices and tech stack fell short of satisfying CMMC controls. By identifying what controls and specific objectives were out of compliance, we developed strategic solutions to remediate them. Starting the remediation process with an overall plan for the firm to work from, we provided guidance to the firm's team members towards best practices, proper initiatives, how to satisfy controls, and other vital compliance fundamentals.

Remediation and implementation continued with technology-agnostic recommendations to maximize their existing investments to obtain CMMC readiness and constructing remediation strategies, including changing policies, procedures, evidence collection, and documentation. By establishing new practices for future compliance satisfaction, the organization was empowered to manage their own compliance program from now on. This was reinforced by providing training on CUI and how to handle it, scoping CUI assets, and general cybersecurity hygiene.

Support efforts also included acting as a knowledge base for them if they had any question on controls or change in their environment and how that could affect their CMMC certification process. With remediation and implementation complete, the organization was prepared for a C3PAO assessment with anticipations of our consultants also providing pre-,during-, and post-assessment support. As part of our advisory efforts, the organization was then introduced to a C3PAO to consider for their assessment when they chose to start engagement.

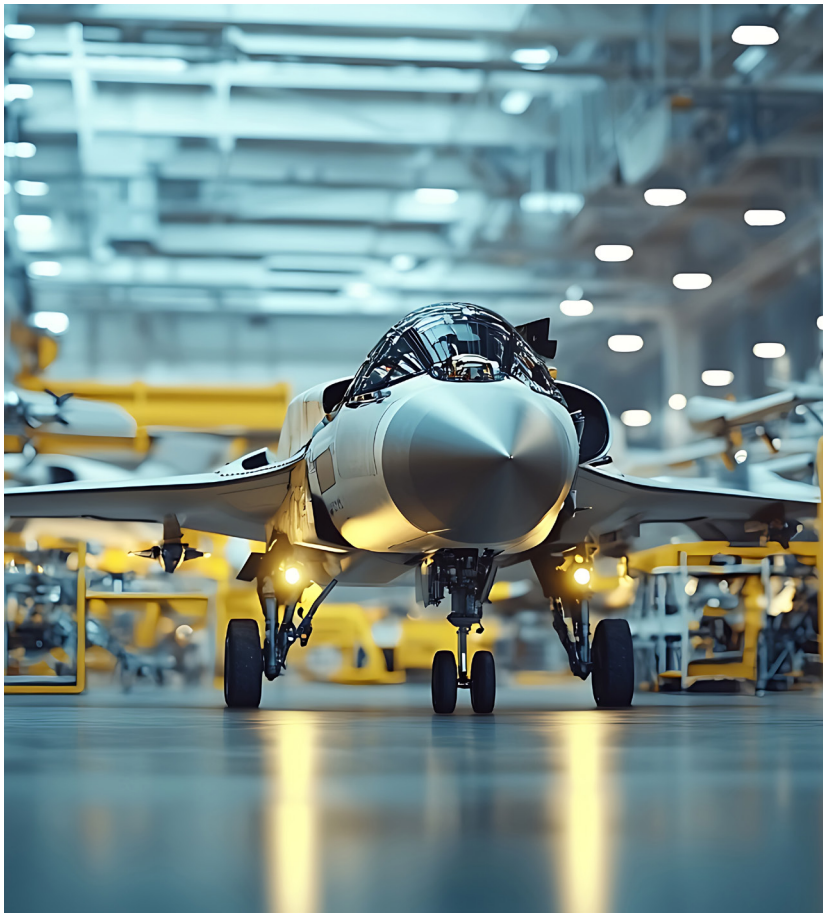
Continued

The Results

This major aerospace engineering partner didn't just get compliant. They became cyber mature. Our team supported the firm's effort to secure their own supply chain and educate them on the impacts of CMMC.

This led to their compliance program development and maintenance moving from an afterthought to a core part of operations.

And most importantly – this organization is now prepared for a C3PAO assessment when they choose to engage in one. This paired with their ongoing, established cyber compliance hygiene practices ensures they won't just pass their assessment, but successfully and proactively maintain their certification status. With CMMC officially going into effect on November 10th, they are officially ahead of the curve on CMMC readiness.



THE CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO

About SP6

SP6 is a niche services firm with expertise in both Security Analytics and Cybersecurity Compliance. In the field of Cybersecurity Compliance, SP6 provides consulting expertise with NIST security frameworks such as NIST CSF, 800-171 and 800-53. These services include security and compliance gap assessments, remediation advisement around missing or failed security controls, outsourced Compliance as a Service, and more.