



SENTINELBLUE

Cybersecurity & Compliance for DIB Manufacturers

SECURITY & CMMC EXPERTISE BUILT FOR THE SHOP FLOOR

Defense manufacturers handle CUI in environments most IT providers were never built for, with legacy machines, shared workstations, and decades-old networks. For small and mid-sized machine shops, the job of meeting NIST SP 800-171 often lands on one person who already wears multiple IT hats.

With years of experience in DIB manufacturing, Sentinel Blue brings the hands-on knowledge to secure your operations and prepare you for CMMC Level 2 without slowing down production.

One Partner for IT, Security, and Compliance

Many machine shops have already tried local MSPs and commercial providers, only to find they lack federal-grade tooling or experience with shop-floor realities like USB transfers to CNC machines, IoT blind spots, and printed CUI.

Sentinel Blue brings IT, security, and compliance together under one roof. We know replacing every legacy system isn't realistic, so instead we determine what can be segmented, removed from the network, or configured to operate securely, so you can meet requirements while keeping critical equipment running.

Why Sentinel Blue

- Hands-on experience in machine shop and precision manufacturing environments
- Solutions scaled to SMB budgets, with big-ticket needs identified early
- Minimal disruption to production
- Friendly, responsive help desk support for small teams





Security That Doesn't Stop at Certification

Your CMMC certification is a milestone, not a finish line. Our Overwatch SOC team monitors your environment around the clock, [catching threats](#) like phishing and malware downloads before they cause damage. Meanwhile, our Pathfinder team helps you maintain compliance through future assessment cycles and plan strategically for what comes next.

BENEFITS FOR MANUFACTURERS

- **GCC High Migration:** Transition from on-premises infrastructure to a secure cloud or hybrid environment aligned with CMMC requirements.
- **Legacy & OT Risk Management:** Segmentation, VLANs, and isolation strategies for industrial machines and legacy systems that can't be replaced.
- **Network Hardening:** Redesign of flat networks built up over decades, plus replacement of aging infrastructure like network switches.
- **Continuous Security Monitoring:** Around-the-clock threat detection and response from a dedicated SOC team with deep DIB expertise.
- **vCISO Advisory & Gap Analysis:** Risk roadmaps, clear milestones, tabletop exercises, and budgeting guidance tailored to your business.
- **Change Management Support:** Expert advocacy that helps security changes get adopted across your org.
- **Security Awareness & Response:** Employee training plus company-wide workflows for reporting incidents.
- **Assessment Readiness & Ongoing Compliance:** Preparation through your CMMC Level 2 assessment and support through future assessment cycles.



Most MSSPs that deal with CMMC environments have never experienced the challenges of a machine shop. Their idea is to just update your machines so they can run the right software, but that's not always possible... Having Sentinel Blue explain all the technical details and how they apply to our environment was the support we needed when we were drowning."

– Amanda Webb, ISSO, Level 1 Fasteners

About Sentinel Blue

Sentinel Blue is a CMMC leader and managed security service provider bringing the power of enterprise cybersecurity tools to federal contractors of all sizes. Specializing in emerging technologies and digital transformation, Sentinel Blue offers comprehensive, scalable, end-to-end cybersecurity solutions for clients and partners within the Defense Industrial Base and other highly regulated industries. [Learn more here.](#)