SENTINELBLUE

Cybersecurity & Compliance for IT Defense Contractors

CYBERSECURITY & CMMC EXPERTISE FOR IT FIRMS IN THE DIB

Defense contractors that deliver IT services to the DoD must be CMMC-certified to keep winning contracts, but many lack the dedicated resources to achieve compliance on their own. Sentinel Blue gives defense IT providers a single partner for compliant GCC High and Azure Government architecture, continuous security monitoring, documentation, vCISO advisory, and more.

A Force Multiplier for Lean IT Teams

Building an enterprise-grade security stack isn't realistic for most small IT teams. Sentinel Blue fills in the gaps with a fully managed program that includes advisory services for leadership and change management to support new systems, tools, and workflows.

On the security side, the program offers continuous monitoring, vulnerability scanning, threat detection, and ongoing SOC incident response. On the compliance side, it includes everything from handling SSP development and POA&M management to presenting documentation during your CMMC assessment.

Sentinel Blue also offers a co-managed option that complements your existing in-house efforts, adding specialized security and compliance expertise and expanding your capacity without replacing the people and processes you rely on.

Why Sentinel Blue

- Security that keeps pace with your new tools, models, and technologies
- Compliance built into your architecture
- Hands-on support from preliminary scoping through assessment day
- vCISO guidance that translates business goals into practical IT decisions

Security Architecture That Supports Your Business

Every IT provider's environment is different, and compliance shouldn't come at the cost of how your business operates. Sentinel Blue works collaboratively with your team to understand the workflows you already have in place and the technologies you'll need to reach your business goals. From there, we build a compliant architecture designed to support your operations today and scale with your future growth.

BENEFITS FOR IT PROVIDERS

- **GCC High & Azure Government Implementation:** Deployment of a compliant cloud enclave with clearly defined boundaries.
- **Environment Assessment & Cleanup:** Review of devices, user accounts, and software to identify what's compliant and what needs remediation.
- **Continuous Security Monitoring:** Around-the-clock threat detection and response, backed by endpoint protection, identity and MFA management, and vulnerability scanning.
- **Compliance Documentation:** SSP development, risk registers, pre-assessment evidence packages, and more.
- **vCISO Advisory:** Strategic guidance that translates business goals into security decisions.
- **Assessment Readiness & Ongoing Compliance:** Support from preliminary scoping through your CMMC Level 2 assessment and future assessment cycles.

> "It's been a huge weight lifted to feel like I'm not by myself, I'm not in this alone... When I have questions about whether something new will comply with CMMC or how I should navigate it, the team is right there. I'm recommending Sentinel Blue to everyone I know that's in this space and having similar challenges."
>
> **– Debra Hill-Cherry, CIO, PSI Pax**

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.**