SENTINELBLUE



Cybersecurity & Compliance Built for the Space Mission

MANAGED SECURITY & CMMC SERVICES FOR AEROSPACE

Aerospace and space companies often serve defense, civil, and commercial customers at the same time, juggling DoD and NASA contracts that each carry their own security and compliance expectations. As security threats multiply, protecting CUI under NIST SP 800-171 and preparing for CMMC Level 2 is only part of the picture.

Sentinel Blue gives aerospace organizations a single experienced partner for compliant cloud environments, continuous security monitoring, and CMMC guidance built around how space operations really work.

Secure from the Ground Segment to the Galaxy

Threats to the space sector extend well beyond the spacecraft, spanning mission systems like command and control, business systems like enterprise networks and software, vulnerable ground facilities, and the supply chain.

To secure this distributed threat environment, Sentinel Blue segments ground and mission infrastructure from enterprise IT. We tightly control and monitor vendor and third-party access, with a SOC team that provides continuous monitoring for your environment and responds to incidents before they disrupt operations.

Why Sentinel Blue

- Deep experience protecting CUI and improving security across the DIB
- GCC High licensing and implementation from a single partner through Microsoft's AOS-G program
- Hands-on support from preliminary scoping through assessment day
- Continuous monitoring from U.S.-based SOC

Strategy That Keeps Pace with the Mission

Beyond day-to-day protection, Sentinel Blue builds and maintains your compliance program, from SSP development and POA&M management to evidence preparation for your CMMC Level 2 assessment. Meanwhile, our vCISO advisors help turn your security posture into a business advantage with risk-based roadmaps and planned security investments ahead of new contracts, sites, and technologies.

BENEFITS FOR AEROSPACE COMPANIES

- **GCC High and Azure Government Implementation:** A compliant cloud environment with clearly defined boundaries that keeps CUI protected and compliance scope manageable.
- **Mission & Enterprise Network Segmentation:** Clear separation between ground station, communications, and mission infrastructure and day-to-day business systems.
- **Secure Remote & Distributed Access:** Identity, MFA, and endpoint controls for engineers, radio operators, and staff working across multiple sites.
- **Continuous Security Monitoring:** Around-the-clock threat detection and response from a SOC team with deep DIB expertise.
- **Unified Compliance Program:** Support for CMMC Level 2, including SSP development and POA&M management, with an understanding of overlapping DoW and NASA regulatory requirements.
- **Supply Chain & Vendor Risk Management:** Guidance on managing the security of your suppliers and providers.
- **vCISO Advisory:** Strategic guidance that aligns security decisions with your mission, contracts, and growth plans.
- **Assessment Readiness & Ongoing Compliance:** Support from preliminary scoping through your CMMC Level 2 assessment and future assessment cycles.

> Sentinel Blue has taken the time to actually understand what we're building, so they're already thinking a step ahead with us. As we onboard new technologies and develop new models, we can work together so the probability of success is higher from day one.
>
> **– Oscar Mancia, Executive Vice President, Ignite Digital**

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.**