Sentinel Blue Marks Milestone Supporting 20 Defense Contractors Through Successful CMMC Level 2 Assessments

Milestone reinforces Sentinel Blue's position as a leading managed cybersecurity provider helping defense contractors achieve CMMC Level 2 certification.

WARRENTON, VA, UNITED STATES, March 6, 2026 /EINPresswire.com/ -- Sentinel Blue, a leader in managed cybersecurity and compliance solutions supporting the Defense Industrial Base, today announced the 20th successful Cybersecurity Maturity Model Certification (CMMC) Level 2 certification of a client on Sentinel Blue's flagship Shield Program. Through the first 14 months of the CMMC program, 20 different defense industry organizations have achieved a CMMC Level 2 (C3PAO) certification through the Shield managed cybersecurity program, not self-assessments, but third-party (C3PAO) certification. The milestone reflects Sentinel Blue's proven methodology for enabling defense contractors to operationalize security, achieve CMMC Level 2 certification, and sustain compliance over time.

> "We're incredibly proud of the achievement; 20 certifications completed is just the beginning for us, but it's a great milestone to celebrate and reflect on." said Andy Sauer, CEO of Sentinel Blue."
>
> *Andy Sauer*

The Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) program requires defense contractors to demonstrate that they have implemented the cybersecurity practices necessary to protect Controlled Unclassified Information (CUI). As the DoD continues phasing CMMC requirements into solicitations and contracts during Phase 1 implementation (November 2025 through November 2026), organizations across the Defense Industrial Base (DIB) must demonstrate implementation of the security practices defined in NIST SP 800-171. Achieving CMMC Level 2 certification signals that a contractor has operationalized and sustained the cybersecurity practices required to protect CUI and compete for DoD contracts that require verified cybersecurity maturity.

"We're incredibly proud of the achievement; 20 certifications completed is still just the beginning for us, but it's a great milestone to celebrate and reflect on." said Andy Sauer, CEO of Sentinel Blue. "The CMMC Certification process is difficult, robust, and demanding on every team in our company and in our partner companies. The milestone comes as the result of years of learning,

of pushing the envelope, putting in sweat equity, and working through challenges. It exemplifies our core value, “Earn It”, as we and our partner companies have surely done. But, as stated, this is still just the beginning for us. We look forward to achieving even more over the remainder of this year! We’re incredibly grateful for the trust our partners have extended to us, and we will continue to earn it, day in and out.”

Sentinel Blue attributes these outcomes to several core elements of its approach. Early engagement with evolving CMMC requirements and active participation across the defense cybersecurity community helped shape the methodologies now embedded within the firm’s Shield program. The program combines structured cybersecurity leadership through Pathfinder, continuous monitoring and response through Overwatch, and resilient IT operations through Vanguard, alongside the security technologies required to protect sensitive defense information. Together, these elements reflect a sustained focus on operational cybersecurity and risk management across contractor environments.

As the DoD continues the Phase 1 rollout of CMMC through November 2026, contractors across the Defense Industrial Base are entering a critical window to evaluate their cybersecurity posture and readiness for certification. Organizations handling CUI, or determining whether they handle it, must assess where they stand today as the program advances toward Phase 2 implementation, when certification requirements will expand further into DoD procurements. Sentinel Blue continues to work alongside contractors navigating this transition, supporting organizations as they implement and sustain the cybersecurity practices required to protect CUI and remain eligible for programs that support national security.

About Sentinel Blue
Founded in 2019, Sentinel Blue is a Virginia-based IT and cybersecurity services firm supporting organizations across the Defense Industrial Base (DIB) and other highly regulated industries. Through its Shield program, Sentinel Blue delivers integrated managed IT and cybersecurity services designed to help organizations build defensible and resilient cybersecurity operations. Sentinel Blue partners with contractors and enterprises to protect sensitive information, meet regulatory requirements, and support national security missions, guided by a belief that enduring security is built through thoughtful leadership, creative problem solving, and a commitment to doing the work the right way.

For more information, visit www.sentinelblue.com or contact Elizabeth Cory at Elizabeth.cory@sentinelblue.com.

Elizabeth Cory
Sentinel Blue
+1 (571) 686-7478
email us here
Visit us on social media:
LinkedIn

YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/897512387

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.