STACK Cybersecurity Achieves CMMC RPO Status

Recognized by Cyber-AB, STACK Cyber is now authorized to support defense contractors with expert CMMC guidance, assessments, and compliance planning.

STACK Cybersecurity logo

LIVONIA, MI, UNITED STATES, May 14, 2025 /EINPresswire.com/ -- STACK Cybersecurity today announced it has achieved Registered Provider Organization (RPO) status under the Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) program. This milestone places STACK among a distinguished group of cybersecurity firms qualified to assist defense contractors as they navigate the growing complexity of DoD compliance requirements.

> Our RPO certification represents our commitment to guiding manufacturers and vendors through cybersecurity requirements so they can attain or maintain their position in the defense supply chain."
>
> *Rich Miller*

[Read related blog post]

RPO status confirms that STACK Cybersecurity has agreed to the Cyber Accreditation Body (Cyber-AB) code of professional conduct, is authorized to deliver non-certified CMMC consulting services, and is now officially listed on the Cyber-AB Marketplace. To achieve this designation, STACK demonstrated a dedicated CMMC practice and employs staff specifically trained in CMMC methodology. This achievement solidifies STACK Cyber's position as a leader in CMMC compliance solutions and services meant to protect defense contractors across the Defense Industrial Base (DIB) and DoD supply chain.

"As DoD requirements continue to evolve, defense contractors face unprecedented challenges in securing their systems and protecting sensitive information," said Rich Miller, CEO of STACK Cybersecurity. "Our RPO certification represents our commitment to guiding manufacturers and vendors through these complex requirements so they can maintain their position in the defense supply chain."

The CMMC framework is designed to safeguard Controlled Unclassified Information (CUI) across the Defense Industrial Base, a network comprising over 300,000 companies. As implementation deadlines draw closer, contractors who fail to achieve certification may find themselves excluded from new DoD contracts.

Rich Miller, Founder and CEO, STACK Cybersecurity

Understanding CMMC: A Critical Defense Initiative

The Cybersecurity Maturity Model Certification (CMMC) framework was developed by the Department of Defense to protect sensitive unclassified information that flows through the defense industrial base. The program addresses the growing threats to the nation's defense supply chain by establishing clear, enforceable cybersecurity standards.

CMMC replaces the previous self-attestation model with a verification-based approach, requiring third-party assessment of contractors' cybersecurity practices. The framework consists of multiple levels of certification, with each level representing an increasing degree of cybersecurity maturity and corresponding protective measures.

CMMC RPO Shield

The importance of CMMC cannot be overstated. It protects an estimated $600 billion in American intellectual property from theft annually. It establishes unified standards across more than 300,000 defense contractors. It enhances national security by securing the entire defense supply chain. It provides clear guidelines for companies of all sizes to implement appropriate cybersecurity controls.

With the Defense Federal Acquisition Regulation Supplement (DFARS) now requiring CMMC compliance for most defense contracts, achieving and maintaining certification has become essential for companies wishing to participate in the defense sector.

A Rare Distinction Among MSPs and MSSPs
What makes STACK's achievement particularly noteworthy is that RPO status remains uncommon among IT Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs). This designation requires proven expertise in federal contracting, rigorous staff training, and a commitment to strict ethical standards.

"Defense contractors, especially smaller manufacturers, often lack the internal resources to navigate CMMC requirements on their own," said Tracey Birkenhauer, CMMC Practice Lead at STACK Cybersecurity. "Our team provides specialized expertise to implement appropriate security measures without overwhelming their budgets or resources."

As a CMMC RPO, STACK Cybersecurity is authorized to provide expert consultation on CMMC requirements, comprehensive gap assessments, remediation planning and implementation, and pre-assessment preparation.

To learn more about STACK Cybersecurity's CMMC services, visit https://stackcyber.com or call +1 (734) 744-5300.

About STACK Cybersecurity:
STACK Cybersecurity is a leading provider of comprehensive cybersecurity solutions for organizations across multiple industries. With a focus on delivering practical, effective security measures, STACK helps clients protect their most valuable digital assets while meeting regulatory requirements. The company is headquartered in Livonia, Michigan, with operations across the United States.

Tracey Birkenhauer
STACK Cybersecurity
+1 734-744-5300
tracey.birkenhauer@stackcyber.com
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube

---

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.