CMMC 2.0 UPDATES: Changes to the Cybersecurity Requirements of DoD Suppliers

written by Lauri Moon | November 19, 2021

Cybersecurity requirements for companies in the DoD supply chain can be confusing. This session will briefly explain the history of these requirements and what we can expect from CMMC 2.0.

Join us to learn how manufacturers can plan, prioritize, and implement cybersecurity requirements in a way that's good for business – now and into the future.

Topics covered include:

- Key changes resulting in the release of CMMC 2.0, building on and refining the original CMMC program requirements
- Updated levels of cybersecurity certification within CMMC 2.0
- New opportunities for self-assessment or third-party audit
- Expected timeline for the rollout of CMMC 2.0, understanding that requirements are still subject to change
- Steps your company can take today to adhere to CMMC 2.0 requirements

Presented in partnership with:

ABOUT THE PRESENTER

Celia Paulsen | National Institute of Standards and Technology (NIST)

Celia Paulsen facilitates efforts to improve the cybersecurity posture of small and medium size manufacturers throughout the U.S. as the National Institute of Standards and Technology (NIST) Manufacturing Extension Partnership (MEP) Cybersecurity Services Specialist. She has been at NIST for about ten years doing research and developing guidance in areas such as cyber supply chain risk

management, small business cybersecurity, and cybersecurity for additive manufacturing. Prior to joining NIST, Celia was an analyst for the National Security Agency in the US Army. She has an MBA in information security from California State University, San Bernardino, and bachelor's degrees in information technology and business management.