CMMC 2.0 is Here - Find Out What It Really Means for DIB and Non-DIB USG Contractors on The Virtual CISO Podcast

The US DoD has just announced CMMC 2.0, a new strategic direction for its cybersecurity program based on public comment and internal assessment.

The Virtual CISO Podcast by Pivot Point Security

HAMILTON, NJ, USA, November 12, 2021 /EINPresswire.com/ -- The US Department of Defense (DoD) has just announced CMMC 2.0, a new strategic direction for its cybersecurity program based on public comment and internal assessment. Many sources are saying that CMMC 2.0 is about "less requirements"—but it's really much more about changing how the DoD will hold defense contractors accountable to the NIST SP 800-171 requirements that have been in place all along.

Since the DoD announced CMMC 2.0 on November 4, 2021, the discussion has focused mainly on what is different and "more relaxed" about the new program: fewer controls, reduced audit requirements, the reinstatement of POA&Ms, and so on. But this is misleading. The reality is that cybersecurity obligations remain largely unchanged for defense industrial base (DIB) organizations.

Further, the DoD's CMMC program is now rationalized as the first instantiation of a wider cybersecurity effort that will shortly encompass all suppliers to the US federal government—and timelines to readiness are likely accelerated versus CMMC 1.0's gradual rollout.

To quickly share everything you most need to know about CMMC 2.0 and the bigger picture it's now part of, Pivot Point Security CISO and Managing Partner, John Verry, recorded a special episode of The Virtual CISO Podcast. Joining John for this show are two of Pivot Point's most senior consultants: George Perezdiaz, CMMC/NIST Security Consultant, and Caleb Leidy, CMMC Consultant/Provisional Assessor.

> If you do business with the US government, don't miss this podcast episode and the sharp analysis it offers."
> *John Verry, CISO & Managing Partner, Pivot Point Security*

Topics discussed include:
- What's new and what's not with CMMC Level 1 (for securing FCI) and what is now called CMMC Level 2 (for securing CUI)
- The overall realignment of the US government's cybersecurity audit program with NIST 800-171
- "Bifurcation" and who will and won't need a third-party audit if you handle CUI
- How CMMC 2.0's new accountability process fits with the recent cybersecurity executive order, the Civil Cyber-Fraud Initiative, the False Claims Act and upcoming rule changes to 32 CFR and 48 CFR
- Why "letters of affirmation" are a boon to SMB security and IT leaders compared to the threat of a third-party audit

If you do business with the US government, don't miss this podcast episode and the sharp analysis it offers.

To listen to this episode anytime, along with any of the previous episodes in The Virtual CISO Podcast series, visit this page.

About Pivot Point Security
Since 2001, Pivot Point Security has been helping organizations understand and effectively manage their information security risk. We work as a logical extension of your team to simplify the complexities of security and compliance. We're where to turn—when InfoSec gets challenging.

Andrea VanSeveren
Pivot Point Security
+1 732-455-1893
email us here
Visit us on social media:
Facebook
LinkedIn