Wondering If You Should Move to Microsoft GCC High for CMMC Compliance? Check out The Virtual CISO Podcast

If you do business with the US DoD, your interest in cybersecurity is probably at an all-time high since the DFARS interim rule went into effect in November.

HAMILTON, NJ, USA, January 5, 2021 /EINPresswire.com/ -- If you do business with the US Department of Defense (DoD), your interest in cybersecurity is probably at an all-time high since the DFARS interim rule went into effect on November 30, 2020. The new regulation mandates that Defense Industrial Base (DIB) companies share a scored self-assessment of their cyber compliance posture with the government prior to any contract award or update, prompting many to look at closing compliance gaps.

The Virtual CISO Podcast by Pivot Point Security

If you're a DIB supplier and you're using Microsoft 365, as so many do, achieving CMMC Level 3 compliance forces some difficult decisions—because the commercial version of O365 is not CMMC compliant. O365 also doesn't comply with requirements around things like incident response and forensic data gathering capabilities set forth in Defense Federal Acquisition Regulation Supplement (DFARS) clauses "c through g," which are almost universal in current DoD contracts… including yours.

Noncompliance or inaccurate self-assessment could put your business on the sidelines for new or updated contracts and/or set you up for legal sanctions under the False Claims Act. Against this backdrop, the choice to migrate to Microsoft Government Community Cloud High (GCC High) looms large and urgent.

To give you the answers you need, the latest episode of The Virtual CISO Podcast from Pivot Point Security features Scott Edwards, President of Summit 7 Systems, one of just a handful of certified Microsoft Resellers of GCC High licensing for SMBs with under 500 licenses. Scott demystifies multiple compliance issues as he explains exactly what CMMC Level 3 (and CMMC Level 1) mandates and how SMBs can achieve this with or without Microsoft solutions.

Topics discussed include:
 CMMC Level 3 compliance requirements and what they mean for users of Microsoft O365, Google G Suite and other email systems
 Who should—and should not—move from Commercial O365 to GCC High
 What the process of moving from O365 commercial edition to the GCC High "government edition" looks like and how much it costs, depending on what data you need to migrate
 Pros and cons of alternatives to moving to GCC High (e.g., encryption overlay solutions like PreVeil)
 A glimpse into the future of Microsoft government and commercial products and features

If your business is looking to achieve compliance with DoD cybersecurity requirements using Microsoft O365 and/or other Microsoft products, this podcast with Scott Edwards provides absolutely ideal background to help you move forward. (It's basically an entire consulting session available for free.)

To listen to this episode anytime, along with any prior 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.

Jeremy Sporn
Pivot Point Security
+1 (609) 495-5290
email us here
Visit us on social media:
Facebook
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/534069322

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.