# Cybersecurity Professionals Say DoD CMMC Strategy Will Not Work--Suggest Alternate Approach ASAP

*They Say Paradigm Shift and a New Solution that Protects Only the DIB is Required*

Turnkey Cybersecurity and Privacy Programs

DENVER, COLORADO, UNITED STATES, May 17, 2021 /EINPresswire.com/ -- A group of experienced cybersecurity professionals has stepped forward to raise the alarm about what they think is a flawed Department of Defense (DoD) strategy to protect the Defense Industrial Base (DIB) from cyber attack.

Chris Golden, one of the founding board members of the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) and Mitch Tanenbaum and Ray Hutchins, owners of Turnkey Cybersecurity & Privacy Solutions LLC (TCPS) are deeply involved in the efforts to protect the DIB. Golden helped organize the CMMC-AB and then build the training program for the original assessors. Hutchins and Tanenbaum have been working with contractors within the DIB for years helping them comply with both the NIST SP 800-171 and CMMC programs.

> I was there at the birth of the CMMC-AB and I feel strongly about its mission. I'm here to say that the mission is threatened and I hope for all our sakes that the DoD responds to that fact quickly.”
>
> *Chris Golden, Founding Board Member, CMMC-AB*

Their hands-on experience in protecting the DIB revealed to them what they believe is wrong with the current DoD approach and they feel fully qualified to question this approach and to bring the issue to the public's attention.

"The current DoD approach does not recognize the urgent state of affairs with respect to cybersecurity within the DIB," says Mitch Tanenbaum, partner and CISO for TCPS. "DoD's current approach does not attack the core issues that must be overcome to secure the DIB. And the current approach is slated to roll out slowly over a period of years while our adversaries run amok in our systems."

Tanenbaum goes on to say, "The underlying, main problem is that DoD provides no real material or financial support to our folks engaged on the front lines of this DIB cyber fight--the CMMC-AB, the CMMC Center of Excellence (CoE) or the DIB companies themselves. If we are really in a DIB cyberwar, then the warriors need real support--and they are not getting it. "

"We know that some primes are trying to set up self-contained, cloud environments for the subs to use. Unfortunately these 'data rooms' do not come close to solving the problem."

But, as patriots and cybersecurity professionals who are passionate about protecting the country's intellectual property, the trio doesn't want to just complain about what is wrong--they want to help fix it. So they spent years analyzing the problem and architecting a solution which they present in their newly released white paper: THE CMMC: NOT THE RIGHT WAY TO FIX THE DIB SECURITY CRISIS -- THERE IS AN EASIER AND CHEAPER SOLUTION DESIGNED TO PROTECT ONLY THE DIB. The white paper requires no technical knowledge to understand. It approaches the problem from a strategic perspective.

"The old way of doing things coupled with a lack of DoD support is not cutting it and is a setup for failure," says Chris Golden. "But we have architected an environment that takes advantage of recent cloud and other technological advances that equate to a completely novel approach to protecting the DIB."

Golden adds, "You can't keep doing what you have been doing wrong for years and expect different results. You've got to channel Elon Musk and think out-of-the-box. That's what we have done and this is what is required to keep existing DIB companies involved with DoD and to attract new, innovative companies to the DIB."

The trio's white paper proposes to use currently operational cloud technologies and creative engineering to fully host and protect DIB companies within multi-tiered, defendable, and agile enclave cloud environments. The basic idea is that DIB companies will be able to migrate their entire current IT infrastructures into a highly structured, standardized, and protected environment. As part of this process, responsibility for IT/cybersecurity/privacy will transfer from DIB companies to the new company.

"This is what we mean by a paradigm shift," says Tanenbaum. "DIB business leadership has zero interest or enthusiasm for managing their IT environments and/or grappling with cybersecurity associated with those environments. It's not their focus nor their core business. If we expect them to protect the data within those systems, we have to help them. They just cannot do it."

But there's more.

The trio makes the claim that their new environment can be engineered to be 100% secure.

"Look, we get it. We are senior cybersecurity professionals with decades of experience. We fully understand the total impossibility of 100% security in today's environment--and even the danger of using such language," says Hutchins. "We are under no illusions about the difficulties, but we urge folks not to think about where we are today--instead, to think forward into the near future. We are there. We can do this. We just have to quit telling ourselves that it's impossible."

Currently the group is building out its management team and has begun the effort to seek DoD or other support to take their engineering to the next level and build the cloud prototype. Then they plan on using the capital markets to fund the complete roll-out of the new system.

When asked how they thought the DoD might react to criticism of its current strategy and calls for radical change, Golden replied, "We are front-line fighters providing feedback to our commanders. We are confident they'll use the information to adjust course as necessary. Plus, the very fact that Michael Brown, the current director of the Defense Innovation Unit (DIU), is being considered by the Senate for the position of Undersecretary of Defense for Acquisition and Sustainment--is a good thing. The nation needs people who understand innovation and he fits the bill. We urge the Senate to confirm him quickly."

Talking about innovation, the team also intends to copy another Elon Musk innovation--sharing their model with others so it can be scaled quickly to the entire DIB.

"We are confident we can successfully solve this problem and make our solution available to the DIB for substantially less cost than is currently being expended. The size of the problem and demand for this type of protection will far exceed our own capabilities," says Hutchins. "Therefore, we plan to share our engineering with others capable of deploying it to the entire DIB ASAP...and then further expand deployment into other commercial markets that need protection."

Mitch Tanenbaum
Turnkey Cybersecurity & Privacy Solutions, LLC
+1 720-891-1663
email us here
Visit us on social media:
LinkedIn

---

This press release can be viewed online at: https://www.einpresswire.com/article/541288336

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.
© 1995-2021 IPD Group, Inc. All Right Reserved.