The "New" CMMC 2.0 (AKA 800-171): Not the Right Way to Fix the DIB Security Crisis

There is an Easier and Cheaper Solution Designed to Protect Only the DIB

by Chris Golden, Mitch Tanenbaum, and Ray Hutchins

AI Statement: This document was written by a human being ***and not AI***. While we may use AI for aspects of our research, we find that AI is (thus far) incapable of writing a document of this kind.

Contents

Abstract: The authors describe why the current CMMC effort cannot succeed and how the technological environment will now support our proposed solution to protect the Defense Industrial Base and other high value targets with 100% security.

Current Analysis

The nation is under active, daily cyber attack by our adversaries. But the nation's response has been too slow and ineffective, resulting in the loss of hundreds of billions of taxpayer dollars and Department of Defense (DoD) intellectual property and weapon systems we all depend upon for our security. A particularly vulnerable segment of our national Defense Industrial Base (DIB) is the huge number (300-750k) of companies that provide critical and sensitive products and services to the DoD--and which remains basically undefended. It is and will remain an enviable situation for

our adversaries.

The DoD has recognized this vulnerability for years and in 2017 moved to require defense contractors to implement cybersecurity controls in DoD contracts via a pledge within contracts by contractors to meet NIST SP 800-171 requirements. Unfortunately, the DoD did not provide

adequate resources to any responsible agencies for enforcement and support. This includes the Defense Contract Management Agency's DIBCAC program, wherein government assessors would travel to a defense contractor's facility and conduct an in-person assessment of their compliance with the controls detailed within NIST SP 800-171. The maximum number of on-site assessments which could be conducted by the DCMA DIBCAC personnel numbered in the dozens per year, wherein well over 350,000 companies required assessment.

Now, the DoD is moving to enhance NIST SP 800-171 requirements with the Cybersecurity Maturity Model Certification (CMMC) program. The new CMMC program attempts to address the issue of enforcement that led to the effective failure of the NIST SP 800-171 program.

Under the CMMC program, DIB companies are no longer able to self-certify their compliance with the government's cybersecurity requirements. The plan is for independent, third-party assessors to perform CMMC assessments on behalf of the government. The government will then leverage the assessment results in order to make contract award decisions. By relying on industry to produce enough qualified and trained assessors, the DoD hopes to conduct over 100,000 on-site assessments per year throughout the DIB. With each CMMC assessment being valid for three years, this number of assessments theoretically should adequately cover the number of contractors resident in the DIB. However, conducting over 100,000 assessments per year, at varying CMMC levels, with differing-sized facilities and the entire range of cybersecurity maturity found within the DIB will take over 5,000 trained and certified assessors to complete. This number goes up in a linear fashion as more and more U.S. government agencies (DHS, GSA, etc.) and cabinet-level organizations adopt the CMMC model as their preferred choice of cybersecurity standard. In addition, all of the third parties that these DIB contractors use and who have access to their data also need to be assessed under the CMMC model.

The movement from a self-assessed cybersecurity requirement to a pass/fail external assessment should make a positive difference, but by itself, even if 5,000 qualified assessors can be recruited and trained in a reasonable amount of time, external assessments are not nearly enough to defend the DIB. This is especially true since (once again) the government and DoD have neither provided nor funded the resources required to achieve DIB CMMC compliance.

There is little evidence that the current approach will succeed--and meanwhile our adversaries are hard at work hollowing out the intellectual property that is the foundation of our nation's security.

The Five Major Roadblocks

1. **Current IT environment available to the great majority of DIB businesses is (practically speaking) ... not defendable.** The vast majority of DIB vendors are small businesses with fewer than 100 employees. Their legacy IT infrastructure environment is far too complex, unstructured, unorganized, and uncoordinated. Systems have been cobbled together over the years by multiple generations of IT personnel and vendors and typically are only

updated when they fail. The resultant hodge-podge of system elements and applications creates an attack surface which is not defendable, assuming rational-sized IT and cybersecurity budgets.

2. **Shortage of qualified technical talent.** Implementing and maintaining IT infrastructure which meets fast-changing business, security, privacy, regulatory and compliance requirements is no easy task. Such an endeavor requires a range of technical and business skill sets that are in high demand and expensive to keep in-house. Developing and maintaining such a workforce is beyond the capabilities of virtually all smaller (and even medium) -sized companies. But without such talent, a secure IT infrastructure is not possible. For example, CMMC Level 3 requires ALL companies, regardless of size, to collect audit logs from ALL relevant systems, analyze those logs, and generate alerts if there is anything suspicious. How many companies have the budget and personnel to do this?
3. **Lack of DIB business leadership commitment to our mission of protecting the country.** Only a small minority of business leaders truly understand the IT infrastructure that their businesses rely upon for their existence. And even fewer have the training or experience to understand cybersecurity. Managing IT and cybersecurity infrastructure is not why they got into their business in the first place, and the only reason they grapple with it is because they have no choice. The great majority of business leadership has no real interest in, or passion for, running a secure IT operation. The DoD hopes to use economics to threaten them into action, and such threats can improve compliance, but the problem is too deep and intractable to be solved without a long-term commitment. Placed in the "or else" position by the DoD, many companies may choose to leave defense contracting altogether, thereby further reducing the capability and cost efficiencies of the DIB
4. **The cybersecurity "protectors" accept no responsibility.** The manner in which current cybersecurity ecosystems are designed and function, cybersecurity vendors and cybersecurity service providers need not accept any responsibility, liability, or risk for the products and services they provide. An IT environment and its security are typically a wide mix of products never designed to work together securely. One failure can lead to others. Therefore, most (if not all) risk remains upon the shoulders of the small, least-defended companies. Even if one vendor is willing to accept the risk for the security of their product, they cannot accept the risk of how a company integrates one vendor's product with those of another vendor--or of an application developed internally.
5. **No IT infrastructure or cybersecurity support from the DoD.** In order for a smaller company to implement an effective cybersecurity program, it needs structure, guidance, content, best-practice processes, pre-vetted tools, government-type cloud environments and - maybe most importantly - mentoring and support via access to competent and informed technical resources (see 2 above). And finally, it needs funding. Such core, structural and cultural change is not inexpensive. Only with this kind of support and funding will smaller companies have a hope of achieving even Level 1 CMMC compliance.

It could be rationally assumed that since the DoD is driving this radical change within the DIB in response to national security threats, the DoD would take responsibility for the current state of affairs and provide the resources required to effect the large-scale change required. Thus far,

however, there is no evidence of that. The DoD does not even fund the CMMC-Accreditation Body or the CMMC Center of Excellence.

If we are accurately describing the current state of affairs with respect to the CMMC, DIB and DoD, then this apparent hands-off approach may end up being the number one reason for CMMC mission failure. And this failure will undoubtedly result in the wasting of billions of dollars spent by DIB private enterprise companies as they futilely chase the wrong cybersecurity solutions. It is our opinion that the current course of action is not only unsustainable but also not cost effective for the DIB. And if not quickly given other alternatives and/or support, many thousands of smaller companies will be forced to leave the DIB because they will be unable to comply with CMMC requirements.

This mass exit may result in the following:

- DIB company compliance requirements reduced temporarily.
- Loss of revenues, leading to more business instabilities and vulnerabilities.
- The nation loses the large, diverse, distributed, source of intellectual firepower and capabilities that these companies represent.
- The original data and IT cybersecurity vulnerabilities and risks of former DIB companies remain.

Note: The solution associated with this White Paper is primarily targeted at the 90% of DIB companies that could be described as “smaller.” In addition, even though larger companies may have bigger budgets, we have seen no evidence that they are significantly more secure than the smaller companies we target.

Solution: An Evolved, IT/Cybersecurity Managed Service Paradigm Specifically for the DIB

Funded primarily by the private enterprise marketplace, we propose to use currently operational cloud technologies to fully host and protect DIB companies within multi-tiered, defendable, and agile enclave cloud environments. The basic idea is that willing companies will migrate their current IT infrastructures into highly structured, standardized, and protected environments. Responsibility for i) IT ii) cybersecurity and iii) privacy will transfer from DIB companies to a newly created services company whose sole mission is to protect and support the DIB.

One such company will be insufficient to protect the full DIB. A series of such organizations will no doubt develop to do so. The first will demonstrate and effectively evangelize the model.

We envision engineering this environment and specific requirements associated with it so it can be replicated by other companies. Demand will far exceed supply. Therefore, following the model established by Elon Musk, we intend to make our solutions available to others who are in a

position to replicate them at minimal cost. We feel this model is required in order to scale at the rate necessary to meet national security demands.
It is our view that it is now technically feasible to protect large swaths of the DIB with extremely high levels of protection and, when done at scale, the costs for such protection will be less than current costs. While development and implementation of such a solution is clearly challenging on multiple levels, we are fortunate that the quickly evolving technical landscape presents this opportunity and solution.

The initial, willing DIB participants, can be migrated and co-located into multi-tiered, defendable, and upgradable enclave cloud environments, versus allowing them to solve this cybersecurity problem for themselves. While such a transition and transfer of risk is no small task, it is less daunting than trying to protect the DIB through the current method of tackling and maintaining CMMC compliance one company at a time.

The creation of multiple secure, government-like (e.g., GCC High), cloud environments which allow for multiple company enclaves is not only technically feasible, but also a superior technical and managerial solution. And the economies of scale of such a shared environment will make it a solution everyone can afford. While most companies only track direct IT costs, there are significant indirect IT costs, that, when added to the direct costs, makes this solution even more attractive. Especially for the majority of DoD contractors - small businesses.

It is our judgment that if these new cloud environments all follow and meet our standardized requirements, then these environments can be engineered to be **100% secure**. Please understand that as cybersecurity professionals, we fully understand the current impossibility of a 100% secure environment and the danger of even using such terminology. But we have come to believe that this is an achievable goal.

But we ask the reader not to think of this solution in terms of today's IT ecosystems. We ask you to move your thinking forward and look into the near future.

Current cybersecurity discussions give all advantages to the attackers. And rightly so. The current IT ecosystem is not defendable for the vast majority of organizations. But if the attackers were always confronted by the most sophisticated defenses available, then the number of attackers would be radically reduced, and defenses could be further honed to deal with them.

We believe that our stated goal of 100% security for clients who are willing to migrate their IT infrastructure into these fully controlled environments is technically feasible--even today with classical computing. However, effective use of emerging technologies such as AI, ML, blockchain, and other technologies, coupled with fully managed IT and security environments can further improve the security equation for participants. And, if one considers the exponential potential of quantum computing, then the possibilities for a new security paradigm become even stronger. The one variable that is hard to control is the human being. We will design, build and manage environments that can even deal with the challenge of error-prone human behavior.

All things considered, we believe our proposed solution is the only logical possibility.

Taking the Conversation Further

Some topics for thought regarding our solution:

1) Our solution represents a radical evolution of the existing MSP and MSSP business models. The current MSP/MSSP model is designed to minimize cost, not to maximize security, and there is no incentive for the MSP/MSSP to increase security.

2) This is the only type of system that can keep up with the ever-changing environment. Technology evolution is occurring at a faster pace each day, and the threat vector also continues to change and adapt each day as well.

3) The current environment wherein each company is required to procure, manage, and evolve their own IT infrastructure environment is no longer feasible.

4) Even though multiple, evolved, managed service providers, providing both general IT and cybersecurity support for the DIB represent multiple points of failure and lucrative targets for our adversaries, the advantages of this model heavily outweigh the downside.

5) The economy of scale that could be provided to the DIB represents a significant value to companies throughout the verticality of the supply chain and the US government within that environment.

6) Being concerned with the cybersecurity practices/processes of one entity is much easier, and cheaper, than having thousands of third-party vendors performing these services.

7) This system would remove most human error from the DIB companies and place it squarely in the realm of technical and cybersecurity professionals.

8) Transferring the responsibility to update and adapt systems and processes to just a few associated organizations versus hundreds of thousands of independently managed companies facilitates a completely different security paradigm than we see today.

9) A single (or a few), managed providers with strong ties to the DoD can be informed of, and react to, changes in the threat environment in near real time.

10) As the DoD (and other U.S. governmental agencies) adopt the CMMC program, they will find it much easier to deal with fewer responsible entities who are providing these services to thousands of companies.

11) The CMMC program will need far fewer resources to become successful. Fewer trained and qualified assessors will be needed to certify fewer critical entities. With more assessors now available than currently required, more frequent assessments can be conducted. So, instead of conducting a CMMC assessment once every three years, and not continuously reducing the real risks that take place much more often than three years, the government can assess whenever a trigger in the operational or strategic environment dictates a new assessment--regardless of interval timing.

12) As our adversaries move to take advantage of gaps in our security posture, those gaps can be remediated in near real-time and prevent the exploitation of any vulnerabilities throughout the entire DIB at one time. This shrinks the window of vulnerabilities that our adversaries have to attempt to steal sensitive data from any of the DIB enclaves.

13) It is noted that our adversaries are moving toward a more artificial intelligence (AI) driven model of attacking companies in the DIB. An AI response to this threat is the logical choice. However, AI technologies are new and usually too expensive for DIB companies. Placing significant AI capability into a managed service provider allows for each and every company in the DIB to share the cost of, and benefit from, this emerging technology and always be at the cutting edge of this technology without having to wait for internal AI economies of scale to reach the point of affordability for them.

14) This model takes advantage of the fact above for all emerging technologies. Machine learning and quantum computing are but two of the newest technologies that will have significant impacts on the security of the DIB and the country. We cannot look into the future and guess which new technology will have the greatest impact, but through the leveraging of a single managed provider, no matter what technology, we can quickly and easily incorporate it into the existing infrastructure and provide it to the DIB in a quicker and more cost-efficient manner.

15) Many companies in the DIB already outsource multiple facets of their businesses. Outsourcing is a common and well understood model for these companies and a route they have chosen over other options based on the same factors listed above. It is cheaper to implement, better for them since they do not have to hire employees for these functions, and easier since they do not have the expertise to fully grasp all of the security issues they face. Companies will be more comfortable with a service provider model, and the country will be more secure.

16) As previously mentioned, this new model assumes that we assume all IT infrastructure and cybersecurity risk. Cyber insurance still exists, but since the environment is so demonstrably more secure, rates would be substantially reduced.

17) This is not solely a technology solution; it is also a process solution. A 100% secure cybersecurity defense must consist of a coordinated mix of engineered technologies, processes, and a cooperative/controlled interaction between the entire ecosystem of participants, including the DIB companies, the DoD (eventually expanding to the whole of the US government), and the

service provider.

18) The assumption today is that regardless of your cybersecurity posture, if the attacker wants in, they can get in. That assumption absolutely must change. What does it take to change that? In today's world, that assumption is true. But nothing stays the same--everything changes. It is time to change this paradigm.

For more information about our business plan and progress, please contact:

Mitch Tanenbaum:
mitch@turnkeycybersecurityandprivacysolutions.com Ray Hutchins:
rh@turnkeycybersecurityandprivacysolutions.com

"After the 800-171 or CMMC gap assessments are complete, then comes the mitigation. This is our area of expertise. And we are warning you that the current approach will not work. We must solve this problem like Elon Musk would. We must think out-of-the-box and engineer a creative new solution ASAP.

And we must start behaving as if we are at war--because we are."

--Ray Hutchins & Mitch Tanenbaum

Did you find this position paper of value? Here are some of our other papers.

- IT Infrastructure Monitoring Issues-Making the Best Choice for Your Company
- Secrets of Hiring and Firing vCISOs
- CMMC Compliance-The New Enclave Approach
- The "NEW" CMMC 2.0 (AKA 800-171): Not the Right Way to Fix the DIB Security Crisis

About the Authors

Ray Hutchins and Mitch Tanenbaum own and operate two cybersecurity companies:

- CyberCecurity, LLC
- Turnkey Cybersecurity and Privacy Solutions, LLC

These are veteran-owned, mission-oriented companies providing defensive governance, strategic and operational guidance, and boots-on-the-ground support to organizations that acknowledge the cyberwar and are ready to actively support and engage in risk reduction and value creation.

Ray's and Mitch's wide range of cyberwar experiences with defending organizations all over the world and their ability to articulate this complex technical environment to leaders has established them as "global cyberwar" authorities. Please learn more about Ray and Mitch here: https://www.cybercecurity.com/about/