CYBER DEFENSE MAGAZINE

eMAGAZINE

SEPTEMBER 2023

In This Edition

MORE INSIDE!

Navigating the Uncertainties of CMMC 2.0: An Urgent Call for Clarity

Unpacking the Complexities, Implications, and Future Outlook of the Cybersecurity Maturity Model Certification

By David Brewer, Director of IT/Cybersecurity (Acting), Saalex Solutions, a division of Saalex Corporation

In the hyperconnected landscape of the digital age, where the onslaught of cybersecurity threats is relentless, robust defense mechanisms are crucial. The Department of Defense (DoD) has taken a leap in this direction with the Cybersecurity Maturity Model Certification (CMMC). Yet, with the introduction of CMMC 2.0, a cloud of uncertainties looms, especially concerning the Level 3 requirements. These uncertainties breed discord within the industry, posing significant threats to prime contracts and the overall integrity of the nation's supply chain.

The Challenge of Ambiguity and its Broad Impact

When looking at the ambiguity surrounding the CMMC Level 3 requirements, the issue extends far beyond inconveniencing contractors; it permeates the entire ecosystem within which these businesses operate. Vital infrastructure and sensitive data find themselves in potentially precarious positions due to the absence of clear guidelines.

In the cyber world, where threats are perpetually evolving, ambiguity can be a catastrophic recipe. Contractors require certainty to safeguard themselves and their partners effectively, ensuring robust protection of vital national interests. The present scenario, wherein the details of the requirements remain nebulous, does not allow for such effective security measures to be put in place.

Moreover, the confusion not only causes an operational hindrance but also stokes the flames of anxiety among industry players. The lack of clarity can result in potentially avoidable mistakes, furthering the risk exposure of the entire supply chain.

A Race Against Time Amidst Unclear Directives

The vacuum of precise information or guidelines concerning the Level 3 requirements has precipitated a frantic race against time among contractors. With a summer deadline for Level 3 announced, businesses find themselves in a maelstrom as they grapple with the lack of specifics.

Adding to this complexity, the National Institute of Standards and Technology (NIST) has released a draft revision to the SP 800-171. Revision 3's industry comment session ended on the 15th of July and is looking to have the revision ratified in late 2024 or early 2025. This not only affects the CMMC standard, as Levels 1 and 2 are solely based on the NIST SP 800-171 standard, but also increases the number of controls from 110 to 138, introducing new Organizational-defined Parameters (ODP). The Rev 3 standard's introduction of ODP allows for a company to define cost and effort based on their size and budget, somewhat alleviating stress for smaller companies without the budget for high-dollar security infrastructure.

This scenario sets up an alarming situation where businesses are preparing for a certification process that might span anywhere from several months to an entire year. Without definitive guidance, businesses are forced to speculate, leading to increased stress levels and potential oversights that could have severe repercussions. Furthermore, the changes to the SP 800-171 standard present additional challenges, as businesses must now adapt to new controls and guidelines.

Such frantic preparation also eats into valuable resources, both human and financial. The inherent uncertainties can lead to companies allocating more resources than necessary, leading to inefficiencies that strain the entire process. The looming changes to the SP 800-171 standard further compound these issues, making the race against time even more critical.

The Ripple Effects: Concerns over Auditors and Industry Implications

The impact of the delays and uncertainties extends far beyond the immediate circle of the contractor community. It causes ripples throughout the cybersecurity industry. There is growing concern about the readiness of CMMC auditors and the quality of training they receive. With the forthcoming new requirements, there is apprehension regarding the auditor's preparedness and the effectiveness of their assessments.

Moreover, in the face of the upcoming new requirements, there's concern over the time and costs associated with maintaining compliance. Companies find themselves in a tight spot, balancing the need to safeguard prime contracts while also managing the financial strain of adhering to the new requirements.

This situation, combined with the uncertainty surrounding the future, could potentially compromise national security. The risk of slowing down the certification process might disrupt the nation's supply chain, leaving it vulnerable to cybersecurity threats.

A Glimmer of Hope Amidst Uncertainty

Despite the prevailing uncertainties, recent developments offer a glimmer of hope. The submission of the proposed CMMC framework to the Office of Management and Budget (OMB) for review is one such silver lining. This step officially kick-starts the final rulemaking process, a crucial milestone indicating progress is being made towards defining and implementing CMMC 2.0.

However, the sense of anticipation that comes with this development is tempered by the fact that the review process can take up to 90 days or longer. And despite the final rule's submission, the final shape it will take remains uncertain, keeping the industry on tenterhooks.

The Waiting Game and Potential Outcomes

Even with this step towards finalizing the CMMC rules, a substantial degree of uncertainty lingers. The review period could go on for months, and the final outcome remains in the realm of the unknown. However, the fact that a consensus on a final rule has been reached and that the framework has been submitted for review suggests that the formal introduction of the latest version of CMMC is on the horizon.

The next steps could see the rule published in the Federal Register under one of two classifications. If published as a proposed rule, it could take a significant amount of time to get to the finish line, potentially taking the better part of a year. However, if the office agrees to publish CMMC as an interim final rule, the rule could take effect over the following 60 days, allowing the CMMC to hit DoD contracts soon after.

Implications for the Future: An Urgent Need for Clarity

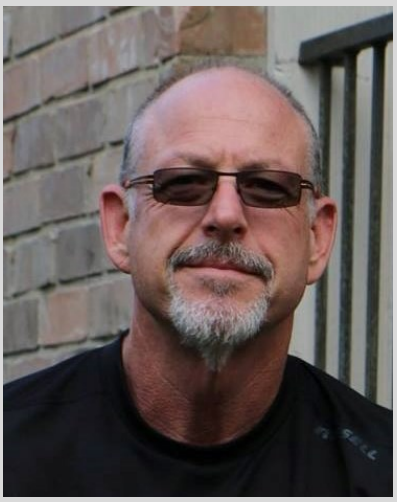
Despite these advancements, the intricate details of the program remain a mystery, casting a long shadow of uncertainty over contractors who handle the Pentagon’s sensitive information. As the industry navigates this ever-evolving landscape of cybersecurity, the ongoing discussion surrounding CMMC 2.0 underscores the critical need for clear, consistent guidelines.

Given the gravity of the situation, there is an urgency for all parties involved – from contractors and auditors to the DoD – to unite in their efforts. By working together, they can navigate these uncertainties, overcome the hurdles, and ensure the integrity of national security. The future success of CMMC 2.0,

and thus the fortification of our cybersecurity defenses, depends on the clarity of guidelines, effective communication, and the collective will to navigate this challenging landscape. This collective effort is needed to ensure that the process is as smooth as possible, and the disruptions caused by these uncertainties are minimized.

Indeed, the road to CMMC 2.0 is fraught with challenges. Yet, by focusing on fostering understanding, unity, and clarity, the industry can overcome these hurdles and fortify our nation's cybersecurity framework. This journey is not merely about achieving certification; it's about shaping the future of cybersecurity in our nation's defense apparatus, ensuring the integrity of our supply chain, and preserving our national security.

About the Author



Dave Brewer is an accomplished information technology professional with over 20 years of experience in IT and cyber security. He currently serves as the Program Manager and acting Director of IT/Cyber Security at Saalex Solutions. Previously, he held positions as Network, VoIP/VTC, Hardware Operations Manager at Peraton and Director of Operations at Hoyt Communications Inc. Dave is pursuing a degree in Information Technology - Security at Western Governors University and boasts an extensive array of certifications, including CompTIA Network Plus, Security Plus, ITIL Foundation, BICSI RCDD, and various CCNA and CCNP certifications. With a recent Cisco Certified Specialist in Data Center Core, Dave's expertise in both management and technical roles has solidified his status as an industry leader. His unwavering commitment to professional development reflects his dedication to staying at the forefront of technological innovation.

David can be reached online at david.brewer@saalex.com and at Saalex's website https://www.saalex.com/.