CMMC Levels 1-3: Going Beyond NIST SP-171

Featuring Katie Stewart as Interviewed by Andrew Hoover

Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

Andrew Hoover: Hi, my name is Andrew Hoover. Welcome to the SEI Podcast Series. I lead the Resilience Engineering Team in the Software Engineering Institute CERT Division at Carnegie Mellon University.

I would like to welcome Katie Stewart, also a senior engineer in the SEI CERT Division. Today, we are here to talk about the Cybersecurity Maturity Model Certification, more commonly known as CMMC. Our discussion is going to focus on CMMC Levels 1-3 and going beyond NIST 800-171.

Let's start off by telling our guests a little bit about ourselves and our backgrounds and what brought us here to the SEI. Like I said, I am Andrew Hoover, and I have been at the SEI for eight years now, primarily working in the Cyber Risk and Resilience Directorate. My background is in cyber auditing and technical vulnerability assessments. I've been able to continue that work here at the SEI performing and building assessments focused on cybersecurity architecture and measuring the resilience of specific systems and services. Katie?

Katie Stewart: Hi, I'm Katie Stewart. I have also been at the SEI for about seven years now, primarily focused on cybersecurity risk and resilience as well as measurement and analysis. Like Andy, I am one of the architects of the CMMC.

Andrew: For members of our audience who are new to this topic, we have done blog posts and webcasts that provide an overview of CMMC and our work on it. We will include links to those in our transcript of this podcast today.

Let's go ahead and talk more about the model. The Cybersecurity Maturity Model Certification, or CMMC, is a capability maturity model being developed and implemented for the Department of Defense [DoD] that defines specific practices across five levels of maturity while also measuring the degree to which those practices are institutionalized within an organization. The DoD will require a CMMC certification for all companies in the Defense Industrial Base [DIB] in order to be awarded a defense contract.

Katie, do you want to tell us what is different about the approach that the CMMC brings compared to the way this is being done today?

Katie: Today, DIB companies that handle or are going to handle controlled unclassified information, or CUI, are required to self-attest that they are meeting the requirements laid out in the Defense Federal Acquisition Rule Supplement, also known as DFARS, which requires compliance with NIST Special Publication 800-171. So, when CMMC is fully implemented, DIB organizations will be assessed by a third-party organization against the CMMC requirements. This will include all of 800-171, like it does today. But it also includes, at Levels 1-3, an additional 20 practices as well as a process maturity component. Today, we are actually going to talk through what those differences are.

Andy: OK, Katie. Thanks for explaining those differences. Earlier we brought up this concept of the CMMC measuring institutionalization. Can you explain that to us and tell us how institutionalization relates to process maturity?

Katie: Sure. If you look at the CMMC there are five defined levels of process maturity. Today, I am just going to talk about Levels 1-3, but we will link to the other material that we provided before that will go into more detail if you are interested in Levels 4 and 5.

Let's start with a high-level view of process maturity. So, what is it? Process institutionalization is achieved through implementing practices that lead to process maturity. Process maturity represents an organization's commitment to and consistency in performing these processes. Measuring process maturity can determine how well an organization has defined, executed, and how they are managing their processes. So, a higher level of process maturity will contribute to more stable processes. More stable processes produce consistent and expected results over time. In addition, and it is very important, more mature processes will be retained during times of stress. This will enable organizations to both better prevent and, in the event of a cyber attack, respond more quickly and easily.

Within the CMMC, formal process maturity is assessed beginning at Level 2. A Level-2 organization is expected to have documented practices that are guided by an established policy.

The documented practices will ensure that the activities are repeatable and consistent. The policy will represent the organization's commitment to the importance of the activity.

At a Level 3, an organization is expected to manage and resource their activities according to a defined plan. This plan ensures that the resources are available to carry out the objectives that were defined in the policy at Level 2. With that, you will have the policy, and the practices and the plan, and they should all be in alignment. The Level 2 and Level 3 process maturity components within the model apply across all of the technical practices being implemented within CMMC. We believe this is actually a fundamental shift. As I talked about before, the current compliance-focused approach relies on self-attestation. So, we should see a shift in organizational culture that will begin to appreciate and recognize the importance of cybersecurity within the DIB.

OK. So, that's process maturity within the CMMC. Now let's take a deeper dive into the other side of the model, which is the cybersecurity practices. Andy, can you give us a quick overview of how the practices are laid out?

Andy: Yes, so the CMMC currently defines 17 domains of technical capability, each with five levels of certification and a number of leveled practices. Most organizations—the DoD thinks probably around 80 percent—will only need to achieve Level 1, which has 17 practices and demonstrates basic cyber hygiene. Before any organization can perform work with CUI, or controlled unclassified information, they will need to have a CMMC Level 3 certification. At Level 3, the certification requires achieving all 130 leveled practices within Levels 1 through 3 of the CMMC.

Katie: OK. So, you said 130 leveled practices. We know that NIST 800-171 has only 110 security requirements. Can you tell us some additional information about the 20 that are included in CMMC?

Andy: Twenty additional practices were added, in addition to those from 171, at Levels 2 and 3 across 9 of the 17 CMMC domains. Seven of these requirements were added to CMMC Level 2 and 13 to Level 3. In addition to protecting the confidentiality of CUI data, the DoD wanted a model that would change organizational behavior to be more security conscious. The CMMC meets that objective by adding practices to those that are already included in 800-171 to ensure that an organization has a well-rounded security program. Then, by institutionalizing all of these practices through the implementation of process maturity, which you already talked about, Katie.

The 20 delta practices can be grouped into three buckets. The first bucket is fundamental practices that were added to the model to assist DIB companies with progressing their cybersecurity capabilities. These are fundamental, no-additional-cost practices that provide

stepping stones of technical progression within the model. There are six practices in this group, which include activities like reviewing audit logs or detecting and reporting events and defining procedures for the handling of CUI data. Again, very basic, fundamental things that we do not anticipate increasing costs for DIB organizations above what is required in the implementation of 800-171.

The second bucket of practices provides increased situational awareness to proactively identify and mitigate risks. This group includes six proactive activities. These are things like performing root-cause analysis as part of your incident-management program. There are a couple of risk management practices that we added and a practice to receive and respond to cyber threat intelligence.

The third bucket of delta practices provides what we are calling enhanced protection and sustainment against common threats to the DIB. These are things like phishing, ransomware, malware. These are targeted, very high-value practices that provide additional protections above and beyond those that are already included in 171 as well as sustainment activities to help organizations recover from cyber events. These practices include things that target phishing, like email forgery and spam protections, performing backups and data recovery, as well as additional controls around managing non-vendor-supported or end-of-life products.

Let's close by talking about the resources that are out there and where they can be accessed. We have already mentioned a few. We have a couple of blog posts that touch on different aspects of the model with a few more in draft, which will be published in the next few weeks. We also have several webinars, fact sheets, and other resources which are all available on our website.

Katie: Once again, thank you for listening to our podcast today. We will include links to all those resources mentioned in this podcast as Andy mentioned. Feel free to reach out to Andy and me directly via email or on LinkedIn. You can also email us at info@sei.cmu.edu. This podcast is available at the SEI website at sei.cmu.edu/podcasts and anywhere you might get podcasts including iTunes, YouTube, Stitcher, and SoundCloud.

Thanks for joining us. This episode is available where you download podcasts, including SoundCloud, Stitcher, TuneIn Radio, Google Podcasts, and Apple Podcasts. It is also available on the SEI website at sei.cmu.edu/podcasts and the SEI's YouTube channel. This copyrighted work is made available through the Software Engineering Institute, a federally funded research and development center sponsored by the U.S. Department of Defense. For more information about the SEI and this work, please visit www.sei.cmu.edu. As always, if you have any questions, please don't hesitate to email us at info@sei.cmu.edu. Thank you.