Developing an Effective CMMC Policy

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. Welcome to the SEI Podcast Series. My name is Andrew Hoover. I lead the Resilience Engineering Team in the Software Engineering Institute's CERT Division at Carnegie Mellon University. I would like to welcome Katie Stewart. Katie is a senior engineer in the SEI CERT Division.

Today, we are here to talk about the process-maturity requirements in the Cybersecurity Maturity Model Certification, or more commonly known as the CMMC. Specifically, today we are going to talk about how to build a good policy.

Let us first start off by telling our guests a little bit about ourselves and our backgrounds. I have been here 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 have been able to continue the assessments work since I have been here at the SEI, performing and building security assessments focused on architecture and cybersecurity resilience. Katie?

Katie Stewart: Hi. As Andy said, I am Katie Stewart. I have also been with the SEI for about seven years now. I am primarily focused on risk and resilience management, and I have done some research on metrics and measurement development.

Andrew: OK. So, for members of our audience who are new to the topic of the CMMC, we have done some introductory blog posts and webcasts that provide a nice overview on the CMMC, the model, and just the overall project, and we will be sure to include links to all of that work in our transcript of this podcast. Katie, one of the requirements at Level Two of the CMMC is to develop a policy. Can you tell us a little bit more about the CMMC process-maturity requirement?

Katie: Any organization that is going for a CMMC assessment at Level Two or above, they will be required to have documented policy or a set of policies that cover the entire scope of the CMMC practices.

Andrew: So, developing policies is certainly a best practice that will likely show a very high return on investment. So, can you talk about why this is such an important activity for organizations to do?

Katie: Creating and documenting policy is a way for senior management in an organization to demonstrate their commitment. They demonstrate that they are committed to the importance of the activities that these policies cover. A policy provides clear expectations for the managers and the employees about what is expected for these activities. You generally actually see this commitment when a senior manager actually signs a policy and then distributes it into the enterprise.

Andrew: That is a good point. It sounds like the key here is that the policy is something that comes from senior management as a way for them to set their expectations for everyone else. Can you tell us what are the various attributes that you would be looking for in a good policy?

Katie: There is a handful of things that you will see within a good policy. A good policy will clearly state the purpose. So, *Why is this policy established and what is the intended purpose?* You will also see a policy define the scope. So, *What is the scope that this policy covers*? *Is it an enterprise-wide policy or perhaps just department-wide or maybe this policy is just specific to one information system?*

Andrew: So, one organization could have multiple policies or likely would.

Katie: They absolutely likely would. It just will depend on the size of the organization and how they are structured will basically drive the establishment of policies. Some other things that you will see within a policy [are] the definition of roles and responsibilities. *Who actually is going to carry out the activities that are covered in this policy?* It covers things like who is responsible for it, who you will see performing it, who has the authority over these activities, and who actually owns the execution of the activities. This might be who is actually going to fund the activities.

Another thing you will see, and this is very important, a policy should direct the establishment and implementation of procedures. So, what do we mean by that? A policy should clearly say, *You need to document what you are going to do under the scope of this policy*. So, while you will not actually generally see the activities documented within the policy, there is strategic and senior-level direction to go out and document these activities. Senior management recognizes the importance of documentation, and you will see that within a policy. Finally, the policy should mention or outline any regulatory guidelines that the policy should address as well.

Andrew: So Katie, our IT environments nowadays are very dynamic, and we have to keep up with the changing threats. Any thoughts on how often a policy should be updated?

Katie: Yes, so that is a pretty good question and one that should be driven by an organization's strategic-planning process. I would say at a minimum you are looking at updating your policies or revisiting them yearly. However, to your point which you just said, there may be driving factors that require a more frequent update in a policy. What you will see is more mature organizations, they not only establish their policies, but they also ensure that these policies are being adhered to and, if they are not, they will make the modifications as needed.

Andrew: So, things like organizational changes, changes to the threat environment, those types of things would probably prompt an update to a policy, right, or at least certainly a review?

Katie: Absolutely.

Andrew: OK. Good. So, they are not kind of, *create and forget*. Can you say a little bit more about the CMMC maturity process or processes that require the establishment of policies?

Katie: As I said before, all organizations that are being certified at a Level Two or above for CMMC will have to provide policies that cover the scope of CMMC activities. So, what these policies do is they demonstrate that senior management sponsors and oversees CMMC activities. More importantly, senior management values the importance of CMMC activities. It is important to note that a single policy within the construct of CMMC could be used to cover more than one CMMC domain, or multiple policies could be used to satisfy one CMMC domain. How you organize your policies within CMMC is up to the organization.

Andrew: That is a good point. So, it is probably important to remind our listeners that establishing a good policy is key to a strong cybersecurity foundation.

Katie: Absolutely, it is one of the most important things an organization can do to demonstrate their commitment to these activities. In some of our later podcasts, we plan on talking about documenting practices, how activities are managed, how to measure activities for effectiveness, and then standardize and optimize.

Andrew: It will be great to continue this discussion. Let us close by talking about some of the resources that are out there and where they can be accessed. We mentioned a few here on this podcast and we will be sure to include links to everything in the transcript.

This podcast will of course be available on the SEI website, which is sei.cmu.edu/podcasts and then of course anywhere that you typically get your podcasts, like iTunes, YouTube, Stitcher, SoundCloud, or wherever. As always, if you have any questions, please don't hesitate to reach out at info@sei.cmu.edu. Thanks.

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.