An Introduction to the CMMC Assessment Guides

featuring Andrew Hoover as Interviewed by Katie Stewart

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.

Katie Stewart: Hi, and welcome to the SEI Podcast Series. My name is Katie Stewart, and I am a senior engineer with the SEI CERT Division. I am joined by my colleague Andrew Hoover. Andrew leads the Resilience Engineering Team at the SEI CERT Division at Carnegie Mellon University.

In today's podcast, we are going to focus on the assessment guides for the Cybersecurity Maturity Model Certification or CMMC. But first, we are going to tell our guests a little bit about ourselves and our backgrounds, and what brought us here to the SEI.

So again, I am Katie Stewart. I have been with the SEI about seven or eight years, and I am primarily focused on risk and resilience as well as measurement and analysis. I have been involved with the CMMC project from the beginning. We are really excited to be releasing the assessment guides. Andy, can you tell us a little bit about yourself?

Andrew: Yes, sure. Katie, thank you. I am Andy Hoover. I have been at the SEI for eight years. Most of that time has been spent in the Cyber Risk and Resilience Directorate. I mainly focus on cybersecurity architecture, cyber resilience, and critical-infrastructure protection. Like Katie, I have been involved in CMMC since the very beginning. So [I am] really happy to talk about the assessment guides and happy to release them.

Katie: Great. Thank you. So for members of our audience who might be new to CMMC, we actually have a lot of different podcasts, blog posts, and webcasts that provide a good overview of the CMMC and the work that we have done on it, so we will link all of those resources in our transcript of this podcast.

Let's get started. So, on this podcast and a couple more after, Andy and I are going to walk through and talk about the long-awaited CMMC assessment guides. The podcast today is going to be a very high-level overview. But definitely listen to the future podcasts, and we are going to dive into a lot more detail. So, let us just start with the basics. Andy, can you tell us what an assessment guide is?

Andrew: Yes sure. At a high level, an assessment guide is a document that the assessors are going to use to conduct a CMMC assessment in an organization. That said, it is also a document that organizations should use to prepare for an upcoming CMMC assessment. That way they will know what the assessor is going to be asking, what types of evidence will be accepted, what are the assessment objectives, and ultimately, what are the requirements for the certification that they will be trying to meet. So, assessment guides, in addition to the direct questions, they also include additional information sometimes: maybe scoping information, what types of acceptable evidence will be required, things like that. Assessment guides are by far the most important document an organization can use to prepare themselves for a CMMC assessment.

Katie: Yes, I agree. I absolutely agree. Can you give a little background about how the CMMC assessment guides were developed?

Andrew: Yes, sure. The assessment guides were primarily developed by those of us on the CMMC model team. In addition to that, there was a lot of collaboration with industry. The CMMC accreditation body, of course, was involved, as well as the assessors from the DCMA [Defense Contracs Management Agency]. We went through a number of iterations with the guides, and they have been used several times and in mock assessments and CMMC Pathfinder activities. Then we also leveraged experience here from the SEI. So, some major inputs into the CMMC model were things like the CERT-RMM [CERT Resilience Management Model], of course, CMMI [Capability Maturity Model Integration], the CRR [Cyber Resilience Review] and some of the other derivatives from those products. We leveraged the assessment information used to conduct those when we built out the CMMC assessment guides.

Katie: Yes. It sounds like it was a very collaborative effort.

Andrew: Yes, it was. There is a lot of input with varying viewpoints from different organizations. Now, this is really key to CMMC because when you think about it, CMMC assessments are going to be done on three-person companies all the way up to the prime contractors. We needed to make sure that the assessment guides were accessible to all. So therefore, getting input and viewpoints from folks within organizations of all different sizes was key to the development.

Katie: I think that is a really important point to make, and I know that a lot of work went into making these guides helpful to all organizations regardless of size in cybersecurity.

Andrew: Yes, absolutely. You know, we are going to talk in detail about the assessment guides and their content in our future podcasts coming out shortly.

Katie: So that is good. In future podcasts, we will walk through the details of what is in the assessment guide, the various sections, and how they can be used. For our current listeners, I am sure you are wondering, where [are] the current draft assessment guides?

Andrew: They are going to be listed on the OUSD CMMC website. That is going to be the authoritative source for all the CMMC information. In addition to the model, the appendices, the assessment guides will be listed out there, and we will definitely link to that site in the transcript of our podcast.

Katie: That is a good point to make again; the authoritative source for all CMMC documents, the model, the assessment guides will always be the OUSD website, right?

Andrew: Yes.

Katie: OK. Great. I am really looking forward to digging in to some of the details of the assessment guides in our next podcast, as well as we will do a couple podcasts specifically on the Level 1 guide and the Level 3 guide.

Andrew: Yes. I mean, those are going to be really good discussions. Looking forward to that.

Katie: Yes. Thanks for being here Andy and talking about this work. As a reminder to our audience, we will include all the links we talked about today in the transcript of our podcast. If you have any questions, please do not hesitate to reach out to us. You can get to us through our LinkedIn pages [Katie] [Andrew] or you can email us at info@sei.cmu.edu. Thank you for joining us today.

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.