Securing the Supply Chain for the Defense Industrial Base

Featuring Gavin Jurecko and 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: Welcome to the SEI Podcast Series. My name is Katie Stewart, and I am the technical manager for cybersecurity assurance in the SEI CERT Division. Today, I am pleased to welcome to our podcast Gavin Jurecko. He is the team lead of resilience diagnostics in the SEI CERT Division. Today, we are going to talk about supply-chain risks in the defense industrial base.

Welcome, Gavin.

Gavin Jurecko: Thank you, Katie. I am looking forward to having this discussion with you this afternoon.

Katie: Yes, it should be good. Before we get into it, Gavin, can you tell us a little bit about yourself, your background, and the work that you do here at the SEI?

Gavin: Sure. I have been with the SEI for a little over eight years now working with critical infrastructure and the defense industrial base. Previously to the SEI, I worked in the transportation sector designing communication systems for trains, as well as in the nuclear sector implementing cybersecurity programs for next-generation nuclear power plants that are currently being built in the southern U.S. As Katie said, I work in the Resilience Diagnostics Team here at SEI, and we focus on creating tools to help organizations baseline their operational resilience capabilities and then reporting out on those, of which we will talk about some today as well.

Katie: Great. Thank you, Gavin. Let's begin our discussion by talking about the role the defense industrial base, or the DIB, plays in securing our country.

Gavin: Sure. For those that aren't as familiar with the defense industrial base, it is essentially the worldwide industrial complex that enables research and development as well as design, production, delivery, and maintenance of military weapons systems, subsystems, or even components and parts to those systems to meet U.S. military requirements. People may have heard in the news some of the bigger programs like the F-35 program. We are talking about the organizations that provide the pieces and parts to that. It is estimated that there are around 300,000 to 500,000 organizations within the defense industrial base, and they are considered a piece of critical infrastructure as defined by CISA's guidelines.

Katie: Yes. I mean it sounds like it would be very, very important to secure the DIB supply chain.

Gavin: Yes. For sure. One, there are so many organizations, and they are providing very vital pieces to our U.S. military systems and subsystems, as well as because there are so many organizations, all of them are coming at this from different angles. There are the well-known prime contractors that have a lot of resources. Then a lot of the most vulnerable organizations within the DIB are small- and mid-sized businesses that make up that.

Katie: Yes, can you say a little bit more about that? Why are our small- and mid-sized businesses more vulnerable?

Gavin: I think it is because they have limited resources. A lot of the prime contractors have a lot of budget funding to do a lot of the cybersecurity things they need to do as well as the system development they are doing. But these small- and mid-sized businesses focus on producing a specific widget or a piece of software to a larger piece of the puzzle. All their expertise is maybe tied up in developing those software components or widgets that they are providing. Oftentimes they don't have the cybersecurity staff to protect the sensitive data that is pushed to them by the larger primes or even the government. Without those resources to protect themselves, they are going to represent the weakest link in the supply chain because they are receiving the information, and it's a foothold for an adversary to possibly gain into the different programs.

Katie: I think it is important to note that in some of these large contracts, like the F-35 that you mentioned, the supply chain, it could be 20, 30 companies deep, right? We are talking about information flow down that happens at many, many levels in the supply chain. Let's dig a little deeper into the problem set. What are some of the challenges that you see in securing this supply chain?

Gavin: Just with our work products that we have here at the SEI, we have identified a number of key challenges that we are helping to solve. The first challenge that we are looking at is the current checklist approach to compliance and maybe how that is being implemented.

Katie: We hear this very, very often that our current self-attestation, checklist compliance, it really doesn't give DoD a good idea of how secure the supply chain really is. Can you talk a little bit more about that?

Gavin: Sure. With the self-attestation, we are relying on each organization to attest to a specific set of requirements. As I mentioned before, the smaller-to-mid-sized organizations don't necessarily understand what those requirements mean, so everyone may interpret those requirements differently. What we are trying to help focus the DoD to develop is a repeatable methodology that allows independent parties to quickly baseline contractors against requirements with well-thought-out guidance on what constitutes having met those requirements. By providing this framework, we can help DIB companies identify gaps before official assessments occur, before the government comes in, or before they may pay somebody to come and certify them. These gaps, they are going to be able to take the results from the assessment and then also manage improvement efforts from those tools.

Katie: I think that's critical. We have got to move from this checklist approach to something that's more enduring. I think that's critical if we're going to really drive improvement across the DIB supply chain. You talked a little bit in the beginning about how every organization looks different, this idea of inconsistent capabilities and resources to tackle these challenges. Can you talk a little bit about what we are doing to help DoD meet this inconsistency of capabilities?

Gavin: Sure. A lot of the times, the compliance activities are focused on specific things like confidentiality of sensitive information. The approaches that we are using are really looking at operational resilience. So at a higher level, all the things an organization should be doing to not only protect their data, but if they have an incident, how can they quickly recover from that incident. All of our assessments meet a standard methodology. All of the practices we ask [about], have guidance that's simplified to specify really exactly what organizations should be doing, and even whenever they are ever responding to these practices, giving guidance on what would constitute a, *Yes, this is implemented*, or a, *Yes, this might be incomplete*. So, these tools really help focus DIB contractors on the capabilities they should implement. It's not so much the technical details, but what is the infrastructure at a higher level? The processes, the procedure, the policies, the planning that should be in place that allow them to ingest any of these more detailed requirements and manage them appropriately. Again, once we have that methodology in place, we provide the reporting that is going to allow them to visually represent. They may have an idea of what gaps they have, but after participating in some assessments from us, we are going to provide them a report and visualize all those gaps and give them the tools they need to say, *Hey, this is really where our biggest weakness is. Let's start here*.

Katie: I think that is actually a really key point to make, is that using these tools, we are actually enabling these organizations to manage their improvement efforts. We are no longer just doing a

snapshot in time. By using a framework to guide improvement efforts, these organizations can measure an improvement, show progress, communicate this up to their leadership, and hopefully get the buy-in and funding to get on a continuous-improvement plan. For small- and mid-sized businesses who maybe don't know where to start, I think this is very critical in their improvement efforts.

Gavin: Yes, exactly. We have had the opportunity to, in some of our programs, not only assess an organization once, but what we're finding a year and a half, two years later, these organizations are coming back to us and asking us to re-baseline them. In almost all of the cases, we have noticed a marked improvement in all of the capabilities across our assessments from that year and a half to two years. When I say almost all, there were a couple organizations that were already doing good to begin with, so when we look at the assessment results, they still continued to maintain that high level. There just wasn't as much improvement to go to than some of these other organizations that maybe started at a weaker position.

Katie: Right. No, that's good. Let's talk about enabling DoD leadership to make decisions around the security posture of the DIB. I would think DoD leaders, they need to have a good picture of the current security posture, and I see this as a huge challenge.

Gavin: Yes. It is one thing to have the assessment methodology, but what are we actually doing with that assessment data to create a data-driven approach? Also, this data-driven approach is going to allow us to pivot and identify where we need to supplement our materials or what the weaknesses are. All of our approaches are grounded in the CERT Resilience Management Model or the CERT-RMM, which is a capability maturity model and assessment method that is underpinned by rigorous measurement.

The linkages between controls and risk reduction have often been difficult to quantify, but by taking these practices in these assessment methodologies, we have been able to build a base level of assessment data and start bringing out metrics and measures that identify what practices are most influential and what not. So, for instance, some of the stuff that we found is, with over 600 of these assessments we've done over the last 10 years, we have tried to identify what are the most impactful processes or procedures. What we are finding is those organizations that plan these activities, they affirmatively say, *Yes, we have a plan that states, here is the training requirements*. They establish funding. They have identified tools, or they have policies and directives from upper-level management getting buy-in, and saying, *This is how we're doing these things* oftentimes perform, or across the board perform, 80 percent of the practices we are talking about. For those that don't do the planning function, for those that don't do policy, that number of practices they are actually performing drops down to less than 35 percent across all of the domains we are looking at.

Katie: That alone is just a key insight I think that DoD can use to drive improvement. We can show through the data that we have collected the value of these process-institutionalization activities and how those really do contribute to the security of the DIB.

I want to talk about one more thing. We said in the beginning, the size of the DIB supply chain is somewhere between 300,000 to 500,000 companies. It is an unrealistic goal to say that Gavin is going to go out and assess all 500,000 organizations. How are we addressing this challenge of scaling? What types of things are we doing to address such a large-scale problem?

Gavin: Yeah, it is a problem. To date, some of the data-driven approach that we have, we have a lot of this assessment data, but we haven't automated it. We are currently working at developing some web applications, some repositories that are going to ingest all of this information and come up with these themes, with these visualizations that are always going to be up to date of, *Here is the help of the DIB according to these methodologies we have*. What we would like to do eventually is open this up to maybe self-assessments for voluntary submittal of self-assessments just to increase that reach.

Katie: These tools, these automation efforts that you are developing, will this allow us to see things in more real time? What advantages do you see with this automation?

Gavin: Exactly. The way that we do this now is we have all this assessment data, but when we want to bring in more assessments, we have to go through all of our processes to recalculate everything. What these portals are going to allow us to do is in real time, see what these themes are, see what the data says about the current health of a DIB based on our methodologies.

Katie: It sounds like you and your team are very busy.

Gavin: Yes. There are a lot of challenges that we are trying to get through. There is never a dull moment with trying to come up with these solutions and implement them, so we are busy.

Katie: Looking ahead, what is on the horizon? What are some new innovations that you guys are looking at?

Gavin: We're continuing to refine our data-driven decisions around supply-chain risk information that we're getting. We are looking at updating the assessment methodology. Right now, a lot of our methodologies, we can report out on NIST-800-171, how your organization may look with compliance to that. We are looking at some ransomware profiles that we can pull into that. So if your organization is really worried about ransomware attacks, we are identifying the practices that can be implemented to possibly reduce the ransomware risk that you may have. We are looking at our data-collection strategies to continue to leverage our assessment insights. Again I had mentioned, we are looking at moving our tool into an online data-capture portal

where all of our assessors can upload their information in real time, but eventually depending on the programs we're working with, we'd like to open this up to just any organization. They would get access to our tool and reporting function, and then we would ask [it] just anonymously they can send us their self-assessment data so we can report that up into the aggregate. We don't necessarily care who's using the tool. We care more of what's the organization size look like, what's the revenue stream, stuff like that, so we can start to compare apples to apples. So, if a bunch of smalls want to be compared, we can take the larger primes out of the equation and give them a truer sense of how they compared to their peers.

We're also looking at developing a training program for our assessments to increase our reach. Right now, we facilitate these over a day-or-two period. If we come in person, it's normally six to eight hours. If we do it over Zoom, we break it into two four-hour sessions, but we want to develop a training program to increase our reach. We're going to continue to add data visualization. So, as we're working with leadership in the DoD, what are some of the things they'd like to see? How can we implement that into our dashboards that we're going to be providing? And then also, one of the more interesting things that have come up through some of our assessments is the social-media risk assessment. So how can we create a capability to measure an organization's social-media risk? We are still working through some ideas on how to do that. Obviously, that presents some legal challenges as well, but there has been some interest expressed in that, and we're looking at how we can develop something to get a better picture on that.

Katie: That sounds very interesting and a good path forward against this challenge of securing the DIB.

Gavin, thank you very much for talking today with us about this work. You and your team are doing a great job tackling this challenge. For our audience, we will include links in the transcripts to any resources that we mentioned during this podcast. I would like to thank everybody for joining us. Bye-bye.

Gavin: Thank you.

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.