Making Process Respectable Again: Advancing DevSecOps in the DoD Mission Space

featuring George Lamb, Bill Nichols, and Eileen Wrubel

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.

Eileen Wrubel: Welcome to the SEI Podcast Series. Warfighters in the Department of Defense operate in high-stakes environments where security, efficiency and speed are critical. In such environments DevSecOps has become critical in the drive toward modernization and overall mission success. A recent study led by researchers here at the Carnegie Mellon University Software Engineering Institute examined the state of DevSecOps within the Department of Defense. And that is what we are here to talk about today.

My name is Eileen Wrubel, and I am a technical director here in the Software Solutions Division at the SEI. Today I am pleased to introduce our podcast guests. George Lamb, who is the director for DoD Cloud and Software Modernization in the Information Enterprise Office of the DoD CIO. George leads the team responsible for the DoD Software Modernization Strategy and its associated implementation plan. From the SEI joining me today is Bill Nichols, who leads the SEI's engineering measurement and analysis work. I

would like to begin by welcoming you both to the SEI Podcast Series. Thank you so much for sitting down with me to talk about your work today.

Bill: You are welcome.

George: Thank you, Eileen.

Eileen: I would like to start by talking about the *why* of this study. Why did the DoD want this study, George, and how are you going to use it?

George: That is a really interesting question. It goes back to where we are in our journey. Right now if you look at where the department is, there are still a lot of legacy systems. We have been looking at, *How do we modernize the entire department's IT base*? We started four or five years ago with a really seminal study looking at the software is never done, changing the mindset that we have to do things faster, and that really software is enabling almost like a weapon. It is not this sort of add on, it is actually the tool that we use to go to battle. You can see that in the things that are happening now with Ukraine. There is this information, and the application of information is such a powerful force. We have been on this journey for four years. If you look at the private sector, DORA and Google have been doing a great job with the state of DevOps. So we kind of modeled on that to understand really where we are. It has taken a while to get here.

In terms of maturity, I think now is a really really interesting point to to put a substantial document out on the state of DevSecOps in the department to explain the maturity that we are at and to really position where we need to change from here on. The past couple years were mostly initial ideas, experimentation, pilots. We have done some amazing things in the DevSecOps world, but we haven't transformed the guts of the department. With the new administration in particular, we are looking at much more rapid change. We are looking at adopting a lot of the guidance and turn it into policy. So it is a good time to to lay down the baseline like where we really come from. What are some of the fundamental challenges? And how do we change from a concept into an institutionalized, really a business, of running IT for the department as something that puts weapons into the hands of warfighters very rapidly and at the pace of modern information. I hate to say modern warfare. The way that things are happening in the battlefield is kind of scary. It is kind of fast. We need to have the enterprise to actually react and be part of that change

Eileen: I wish I could remember the source of this quote, but a phrase I have

always loved is, *Agility is the ability to turn on a dime for a dime*. That feels very much to me like what you are talking about. The ability to advance quickly towards our objectives to be able to pivot in the face of changing technology, changing threat environments, and continuously be able to deliver software-enabled capability to the warfighter wherever and whenever it is needed.

George: The only thing I would question is it is not really for a dime. There is a lot of infrastructure. There is of capability that is necessary to make that change happen very quickly. But yes, to move as fast as we can and to have the infrastructure that we can do that securely. If you look at DevOps and how the industry works, DoD is DevSecOps. We don't do anything without understanding what are the implications for our security? We don't want to be callous about that, but we want to have that *Sec* tooling in the middle, as part of the overall infrastructure, so it doesn't slow us down. If it was to be DevOpsSec, that is how it is now, and it doesn't work. But DevSecOps where *Sec* is actually built into the factory, that is a key aspect. That is what enables us to move very quickly.

Eileen: George, can you tell me a little bit about why the DoD chose to partner with SEI researchers to execute this study?

George: That is an easy question. At the CIO level, we know how a lot of the structures work, but we don't have the researchers that are in the programs developing like the SEI does, the intimacy SEI has with a lot of programs and the insight really from the academic and the quantitative perspective. That is what is necessary to turn a strategy document into an insightful document. That is why we really reached out to SEI for that insight and the quantitative expertise to bring data and to bring numbers to bear and not just have a strategy that was kind of, *This is a good thing to do*. We wanted to have that quantification inside of the document.

Eileen: To really integrate those empirical analytical insights with the good software practice and the good security practice right from the start so that we are moving out with executable policy where we understand when we are making progress, and we understand when we when we are hitting our goals.

George: Yes. Data analytics is informing a lot of our decisionmaking. A lot of time it is intuition. We know industry gets a lot of speed out of DevOps. We can see what is happening. But we wanted to get that quantitative basis in here, and at least get the data, so we can make decisions more in the future. That was kind of the the special spin. That was really I think what SEI brought

to the table.

Eileen: Let's talk about the major findings. How would you characterize the present state of DevSecOps in the DoD based on what we uncovered, all the people that we talked to, and all of he analytical backbone.

George: I don't know if you have seen the document. It is going to be out soon. It has a great picture with DevOps in the middle.

Eileen: So excited.

George: The first thing we wanted to do is just capture the success stories because there have been some amazing success stories in DevSecOps that really should be highlighted across the department. We wanted to base it on what have people done right, overcoming all the institutional barriers, the procedural, policy barriers to be successful. So we wanted to get those down. They are across the fourth estate. They are across the services. That is kind of the basis, *What are we doing right?* Then the second big piece was, *How do we turn this into the default way of doing business?* We want more programs to be successful. We want more programs to deliver this rapid capability. The way that we are looking at the software factories in the department, it is actually like a bunch of services. It is not necessarily a centralized organization. Each of the services, the Air Force, Navy, Army, and Space Force Marines [The U.S. Marine Corps Forces Space Command], they are all managing their own software ecosystems. At the CIO level, we put consistency across that. We wanted to understand how they are being managed as business units. So how they are looking at the portfolio of software factories, how they are looking at different aspects of their mission space and applying DevSecOps to all of those aspects of the mission space. That is kind of the transformation that we are seeing right now in the department that we are at that point where we are standing up offices in all of the departments. It is happening naturally. There is a great study by the Navy looking at the state of their software factories and starting to optimize it. *Which ones are being the most effective? Where is their overlaps? Where are there gaps? And how do we move pieces around to cover the entire business base?* You are seeing that across the board. We wanted to to call that out and say that this is really a strategic maturity state that we are starting to manage the business of DevSecOps and information management.

Then we wanted to capture where we see fundamental issues. Things like, *Where is the policy inconsistent? How about the funding models? There are lots of different ways that money flows in the department. Some are more effective than*

others, and how are those funding models applied? How is the resourcing happening? When we try and do a transformation from an old to new, there are a lot of legacy skills that need to be updated. We have to partner with organizations. You have to bring in the third estate. You have to bring in the defense industrial base. You have to bring in small, innovative companies, some of the work coming out of DIU where these startups are coming in. We have to figure out how we are going to change that space. Looking at how the other programs that are successful have done that, that is just fascinating sort of the partnering the lessons learned. That is kind of where the key lessons are. One is that there have been successes. This is the right way to go. We have proven that. It hasn't been institutionalized. We are starting to actually manage it as an institution. We are starting to see the pieces that you need to turn it in.

The other major thing that we are doing from the CIO's office is we are starting to change a lot of the policy that is used to build software. If you look at existing policy, it is still basically encoded for waterfall and the big processes that take many years. We are trying to take all these lessons in the next year—maybe six months to a year; we are moving pretty quickly in this—to change the fundamental policy to mandate this. You can see in the acquisition space, with the Software Acquisition Pathway driving the way that we fund programs, and then pushing that to how we test programs. Instead of testing at the end, testing at the beginning; how we drive cyber across programs once again, understanding the risk management framework and the ATO process driving that into the beginning of the process. There are lots of different pieces so fundamentally changing how the architecture of building software is policy in the department.

Hopefully that answers your question. It has been a busy year trying to see how everything is working. We are not there, but we are understanding in a really good place. It is so exciting. It is like the cusp of transformation going from like a startup into like a real business where we can start delivering the growth models and get a payoff on the dividends we are putting in.

Eileen: Really capitalize on proven practices in these different contexts and different mission spaces to help continue to expand our innovation capacity and our ability to adapt and to pivot.

George: Yes, it is so exciting to go to software factories. They have done incredible work. We really want to just champion the work that has happened in these software factories. You don't see them unless you're in that mission system where they are pushing stuff, the end product. So

putting that visibility out and then using that as example to build policy so we can do more of that across the department.

Eileen: I would like to talk a little bit more about the software factories. We talk in the study about how prescriptive measurements, one size doesn't fit all, we talk about that in a lot of different ways. I would like to focus a little bit on the empirical findings about the behaviors of the software factories in the different mission spaces because I think that what we uncovered there is really going to be important when we talk about the efficiency of these organizations and being able to help leaders identify the appropriate business models and appropriate measurements for understanding the achievement of outcomes. This was really interesting to me what we uncovered here from a quantitative perspective that backs up the insights that we have had.

Bill: That was really one of the things that jumped out at me. George asked at the beginning of this, try to find something, a takeaway, some key piece of information that is interesting from each of these topic areas. Wow. This one just jumped out at us. We looked at several different types of software factories. There were already some categorizations like some of these were primarily made for training, not just the engineers but training soldiers. Some of these were mission critical. Others were really focused on providing the DevSecOps pipeline capabilities as a service and how to stand these up. What we found was there were some subtle differences in the culture. To give you an example, in the in the mission-critical, of all of the DevSecOps cultural attributes, the one that came to the top was leadership. You needed strong leadership. However, when you went to these more educational pipelines, the most critical attribute was learning. Then, when you went to the infrastructure-as-code pipelines, those who were responsible for how to stand these things up, it turned out to be collaboration stakeholder. We realized there is no single way of evaluating each of these pipelines as a group. You have to think about what are their individual goals. These different types of pipelines had clearly different goals. They don't get evaluated quite the same way. That was something that should be obvious in retrospect, but when we looked at it from a cultural perspective, it really jumped out at us.

Eileen: That helps us understand what behaviors and practices are really prevalent, are really strong in different organizations versus where there might be less emphasis on different kinds of activities based on the mission outcomes that are prioritized in those different spaces for those different software factories.

Bill: And it has a profound effect on how you choose leadership for these different types of pipeline. The leaders have to be attuned to what are their real goals, and they have to provide that environment.

George: When Bill talks about leadership, a good example is in the weapons systems or the production systems. The biggest challenge isn't developing the software, it is getting the software into production. You have to really understand how it is going into production, who the end users are, [and] what systems are currently there that need to be replaced or to be migrated out. It used to be people would think the big bang would happen, and all of a sudden a new system appears. That really doesn't work in the department. It has got to be an evolutionary step out, but there are a lot of other stakeholders. That leadership is a lot of understanding what the end impact is, and how do I get it into production?

We see failed systems that don't get into production. It is typically because not that the software or the technology or the process failed, but it is the leadership to manage that change. That one just jumps right at you. We have amazing infrastructure-as-code in the pipelines and folks can do that. That can get into production because it is going to software factories. But pushing the end result of a software factory is getting through to the authorization boundaries. It is really an interesting problem.

Eileen: You talked about the importance of leadership, both of you. There is a great success story. There are a number of success stories that we share throughout the study, but there is one we dedicated significant real estate to, which is the story of [U.S.] MEPCOM, the U.S. Military Entrance Processing Command. For listeners who haven't been through that process, MEPCOM is where we screen and process (medically process) recruits fom all the different processing stations around the country. It is folks who are signing on the dotted line to step into a uniform. That is critical to everything that we do with our defense workforce is actually bringing them in the door to begin with. I am wondering, George, if you could tell us a little bit about the MEPCOM story. Give our listeners a little bit to look forward to when we publish the study about what they can expect to learn.

George: You really hit it on the head. The customers for MEPCOM are high school students and college students who are going to join the military. A very important mission. We base our goals on recruiting from the systems that they use. It was an old system. It was a mainframe system. I think it was built in the '70s, '80s, '90s. It still ran on mainframes. They knew it had to be

changed. It wasn't meeting the goals, but it was so embedded into many other systems that it was really hard to untangle it. There were two tries. Matt Lince, the man that actually wound up being responsible for the MEPCOM transformation, he talks about the two systems that they failed miserably on because they couldn't take it into a production system. There wasn't the authority to take it in. There were too many people that said, *No, this isn't ready. It is too risky*. So that leadership was an important aspect centralizing the decisionmaking. It didn't really kick in until Matt was given the 51 percent vote on any major decisions. It is kind of unheard of in the department where one person has the majority vote on taking into production. But it was so critical for MEPCOM to make this transformation.

The staff that was maintaining the old systems, they were ready to retire. That was the linchpin. Nobody could retire if they didn't continue to modernize. Then the way that he reached out across the board. He came to CIO. He went to the Defense Digital Service to find the best practices. So it was really an understanding of, *What are the options here?* He did very unique things about public private partnerships pulling in small companies that could do DevSecOps that had that expertise, marrying it with the best developers that were in the MEPCOM world. Taking some of the leaders from other key programs and bringing them together. Then when they went into production, they were live with a 24-hour help desk for any problems that happened for the first month of production. It was very focused on, *How do we get this into production?* They knew it was a mission-critical system, so if recruiting stops, it was a problem. The recruiters, they would be online. They would report bugs in. This is another unheard of thing. They would call the help desk. It was open to everyone that had an issue, so everyone could see the remediation happening. They could see the changes happen in effect, and the changes would flow through the pipeline and get into the production system within 24 hours. It was instantaneous change, a beautiful example.

The first system was minimal. The key is minimally viable compliant. It didn't have any of the bells and whistles. It did have the integration, like some of the hard problems, integration to the banking system, integration to the records. But that minimum viable concept was the first piece. The younger users liked it. Some of the people were experiencing all of these capabilities that were missing, but within the first week they stabilized it. Within the first month it was actually running at speed. Then gradually, every month, every release, more functionality came in. That was the big transformation. That is the story I like to take is you have to be able to accept what is there and work with it, but then trust that it is going to get better. That trust is a key part of the leadership, and it continues to get better. They finished that system. It is

completely in production. There were eight systems in MEPCOM. He [Matt Lince] is going on the other systems. A great example of the leadership, the functionality, the right ways to do things. Some of the lessons learned have been published out across the department and just a modernization. It is great to see when it happens. There is a great product out there. The recruiters come in, the high school students. They have something that works on their cell phones. They have something that works in the environments that they are used to. It is no longer going and sitting in front of recruiter on a teletype. It is truly modernized, and it is making a difference in how we staff the Department of Defense.

Eileen: Trust and collaboration are the coin of the realm when we talk about Agile software development, iterative incremental production, we talk about DevSecOps. The choices that they made there, I think, regarding the absolute transparency of the process. It was kind of taking a risk to open up that phone number to anybody and everybody without going through some traditional wickets. That seems to have really built up trust in the process that they are going to continue to deliver on the capability that they promised and continue to bring their stakeholders along with them. The outreach to other leaders to learn about best practices and build different kinds of innovative partnerships really shows leadership that is committed to linking arms and taking a value-oriented perspective to satisfying the goals of all the different stakeholders in the process.

George: It is like throwing away the old way of doing business, adopting a new way. Prioritizing is key. Another fascinating story is they transitioned like 400 necessary bug fixes from the old system into their backlog. When the new system came in they realized that none of those were actually necessary. The new process had fixed all of that backlog, so they got rid of tech debt at the same time. So many like benefits of doing this new approach.

Eileen: That is fantastic.

Bill: To build on what George has been talking about, what I found really fascinating about this experience. Talking to Matt, he is not an IT Guy. To a large extent that is why he was successful. It is kind of counterintuitive that a non-IT guy would be able to drive the success of this program, but he was a professional who was able to find ways to say, *Yes, running into all of these different institutional barriers like, Where do you go for recruiting? How do you get these certain agreements in place?* He knew how to get things done.

That is what we need to do in the DevOps world, figure out how to get these done in this environment. What needs to change? A lot of these aren't necessarily against the rules. But it is not the way we did business, and he was able to find a way to make the other people see his point of view and how to get it done.

Eileen: It sounds like he didn't have a lot of underlying assumptions about how things had to work because this wasn't his prior typical mission space. If you don't have the preconceived notions to begin with, it is a lot easier to climb out away from them.

Bill: And he had the right skill set. He had the skill set you really needed to be successful here.

Eileen: It is fascinating to me that the success story that we really fell in love with because it displayed pretty much every aspect of the journey and lots of great collaboration and just such a strong example of leadership, it strikes me that that that story is effectively about the very first entry point after the recruiter that our DoD workforce has in joining the force. George, you talked about the SWAP study earlier and how it highlighted challenges faced by our software workforce in the DoD. You all see what I did there? I went from workforce to workforce. That [the SWAP study] talked about the need for real specialized software-focused career paths and continuous support for those professionals. I know that we talked in the study about a lot of the strategic efforts that the DoD has has taken on specifically to build and sustain a robust workforce for software and DevSecOps. George, I am wondering if you can tell us about some of those critical efforts and where they stand now.

George: I think probably the most interesting thing, when I got here, there were no software engineers in the department. Engineers were a different category. Looking at the software landscape, we have been working with the folks that code the different job roles and the different capabilities of those roles, and they have transformed how the roles actually exist. So instead of being more of a rigid process, there are now key roles in place, and then there are job categories and capabilities associated with what is now a dynamic list. We can actually build work roles that reflect the skills that are needed. Not necessarily changing the old system but transforming how we think about the skill sets that are involved.

Now we have a much better ability to staff more accurately. That is just within the internal workforce.

The second critical piece is understanding the partnership. If you go to the software factories, one of the key aspects is, it is badgeless. You can't really tell if you are enlisted, if you are civilian, if you are a contractor. Bringing together teams—and this is just a basic, Agile tenet—but in the military, where things are so regimented, it is important to reflect that different kind of skills, both inside the military and outside, are necessary to bring to bear. It is a workforce management, but it is also an acquisition process. *How do we bring in new contractors and have the ability to change people and bring in different skills as things flow through the process and then to have generalists that could be in different roles*? You get someone that is a really good architect on one sprint, and you want to keep them on another sprint. You want to have a particular developer that has a skill and moving between. Because we have many different pipelines running at the same time. Many sprints are running. Things are concurrent. You want to have a lot more flexibility in the acquisition process and sort of the assignment of skills to roles.

I think those are probably the two big things. First is getting rid of the rigidity of how we we sort of categorize people and then bringing in the flexibility to take these new skills that quite frankly don't exist in the department or now they exist, but they are not widespread. And how do we multiply the amount of skills quickly, both through augmenting what we have and then transitioning and mentoring and learning on the job?

Eileen: I am seeing a picture come together where we talked about developing those quantitative and analytical insights about what is happening in the software factories. How are we evaluating progress/process? How are we understanding the connection between engineering activity and the value actually delivered to the warfighter and understanding, when we talk about the business models then for the software organizations, how do they need to be staffed? What kinds of funding do they need to be able to deliver capability in a continuous way, but also to be able to to be able to adapt capacity in the face of new innovation or in the face of changing threat environments or in the face of a changing workforce. With a study of this magnitude, I see so much potential for impact. The impact is really going to be more substantial with actionable insights and actionable outcomes coming out of this to drive future efforts. I am wondering, George, if you could talk about next steps that the DoD is considering to address the questions in the report. We can talk with Bill about all the exciting opportunities for developing and maintaining the

analytical insight to help us understand how effectively we are moving out on those changes towards achieving our goals.

George: Big topics. On the first one, the work that we are seeing across the services. In the Navy, they stood up the new sort of portfolio management office, and they did a really deep dive in DevSecOps. In the Air Force, there is the new software directorate that is looking across all of the manufacturing for airframes: from the fighters to the tankers to the bombers, how all of those fit together. They have sort of brought that under one organization.

There is a a group that is working on the software factory, which is the pipelines and the tools that are consistent across all those. Then the separate software factories that have specialization in each one of those particular airframes. That kind of management we are seeing happening. I think that is very quantitative as we optimize. We look at how the factories are being used, how the platforms are being used. Putting the metrics across a set of factories that are all sort of similar gives us ability to do a little bit more analytics on it. Right now you can't really compare across software factories because every product is so different, every mission is so different. We are getting better datasets there.

The other really big area—and I hear a lot about this in terms of the difference between the Department of Defense and commercial space—is that *Sec* piece. The way in the report we frame it is continuous authorization to operate. CATO is the transformation from traditional authorization, which is very manual and paper-based, into a continuous process where we are using the tooling of DevSecOps, the tooling of actually DevOps, to put the gateways in place to put the promotion, the migration of software as it goes through development into test into production. There is so much analytics in that space. Just using the GitHubs, the GitLabs, the basic tooling gives us incredible insight. In two ways I would point out. One is the process flow through that, to understand how we can get ATO a little bit faster. How we can make it continuous so that someone that is looking at the process doesn't have to look at the end product. They can look at how the product was made, which is actually a lot more insightful. If you understand how the product was made, you feel a little bit more confident, even though the end product is going do a particular function. That process that by making it and by checking every step of the process gives a lot more assurance. That is going to move the ATO process a lot faster.

The second really interesting piece is the supply chain. When we look at building software, there is the factory that makes it, but there are all the pieces that go into that factory: open source, third-party libraries, pieces of existing components that have to be integrated. DevSecOps give us a really good handle on understanding what is coming into the process, knowing what is built into the product, which open source libraries are used. We are working a lot with the CATO, also looking at the RMF [Risk Management Framework] process, which has always been very manual.

The buzzword that I am hearing now is automated RMF, which goes hand in hand with continuous ATO. We are looking at how we accelerate that whole cyber and get that *Sec* piece so it is not something that makes the department much slower or much different, but how it can happen instantaneously, happen more securely. Then what I would actually love to see is the lessons that we have, the insights that we have by securing our pipelines, goes back into the general public, and it starts feeding the the way that software in the United States is built to be more secure overall. Taking lessons learned from the department, quantifying them, putting really good information as to what is the value of this extra *Sec* that we are putting into it. What tools we are using, how we do it through reference designs, and then understanding what the business value we get out of that is. So lots of places for data to be used both in making our product faster and making it more secure and then sharing it and understanding how to manage it as a business.

Eileen: I think in so many of these cases you talked about data existing in the infrastructure. It is there. There could be a tendency to treat it as either as exhaust or to say, *Oh, I have all this data. Let me collect it all without stopping to think mindfully about like there are sort of two ends of that*. And I know, Bill, you have some great thoughts about how we can smartly use the data that we know exists in all of our our development security infrastructure moving forward.

Bill: Absolutely, yes. One of the things that we recommend all the time is you never want to have just one source of data. You need to be able to look at things from a number of different perspectives. As George suggested, it is not just an outcome. An outcome is result of a process. We need to be able to look at the individual processes to understand what they are trying to accomplish and understand are they doing what they expect to do? Are they getting the outputs?

Now one of the nice things about DevSecOps is it has made process respectable again. You have a lot of measurement opportunities in DevSecOps. Our challenge moving forward is to understand what is the information that we can extract from these processes that is going to give us the information and the confidence these products are secure, the confidence that we are going to be able to meet our commitments.

Eileen: I love that you said making process respectable again.

George: We need to make that a tagline. That is a great quote, Bill. I like that

Eileen: I think we are going to start using that in a bunch of places. Sometimes there is a tendency, for folks who don't think about the process around what they build, there can be a tendency to think about executing a process for the sake of executing the process, right? That is when something becomes a checklist as opposed to a way of thinking. The benefits that we see in terms of speed and efficiency and adaptability from adopting DevSecOps processes really does. I love that. I am going to start using that everywhere: make process respectable again. I also think that from what you said, Bill, the insight that we can get now from right from understanding processes—George, you talked about this in terms of supply chain—but a well instrumented process where we are collecting data that we can tie to the achievement of value and the outcomes that we are looking for. That goes all the way back to the trust that our user community needs to have in the folks that are building software, mission software, that it is going to be the right thing in the right time at the right place. The trust that it is going to be secure. It is going do all the things it is supposed to do. It is not going do any of the things that it is not supposed to do. When you put all of those things together, making process respectable again means you get that trust. You get that confidence that, *I am going to have the thing I need when I need it in Ukraine or in Washington or in Boyers Pennsylvania, or San Antonio*.

Bill: Good outcomes should not be an accident. There should be a predictable thread that runs through everything you do to get to that outcome.

George: Yes, it is like when you get patches for your computer. There used to be a day and age when you were worried about it, but now you understand that those patches are necessary. There is some kind of risk that is in there. We need to get to the point where we can take things that come out of the

software factory, and we can run with them confidently.

Eileen: I want to ask both of you, and I will start with Bill this time, we worked together extensively for probably over a year understanding the goals of this study and reaching out to people and collecting information and slicing it and dicing it to really understand the story and put together some recommendations and a playbook for moving forward. Was there anything that really surprised you over the course of this study?

Bill: I certainly wasn't surprised at the commitment we found among so many of the people we interviewed. That really stood out, but that shouldn't be surprising. I think if there was something that was surprising, it was one of the things we learned from the MEPCOM, and that was that it literally was not the technical expertise that made this effective. It was the leadership ability to get things done. I love the way Matt put it. It was finding a way to say yes.

Eileen: I appreciate that. George, you got a little bit of time to think about that since I made Bill answer me first.

George: I did. It is kind of interesting. At the CIO office we know a lot about how things are operating. When we started this, we just asked SEI to go figure it out. We gave you some guidance, but at the end of the day, when you went and figured out you kind of got to the place that we thought we were at. It was a good check that we are that critical transformation. We actually do know what we are doing. It is just a good gut check. In terms of how we got here. I think the process was pretty consistent. We did the DIB SWAP report. Then we did a software modernization strategy. We did a two-year plan. We wrapped that one in '24. Now we are doing the *State of DevSecOps report* to tell us where we are and going back and stating those two years we spent implementing actually are effective. Now, we are starting the next two-year implementation plan. I'm pretty excited about where we are going with that.

In terms of surprises. It wasn't necessarily a surprise, but it was interesting, seeing the SEI come to the same conclusions. We are in a pretty good place. This is a really good story. We were expecting to have a lot more recommendations, a lot more criticism. I think it came out to be a fairly positive report.

Eileen: It did. What really struck me was the ability. When we stood back and and looked at everything, the ability to say, *Wow! We know where the people on*

the leading edge of the change wave, we know where they might still be bumping up against things where they have to be the first mover where there are unanswered questions. But consistently what we saw was that all the efforts that that CIO and the services were moving out on indicated that the leadership in the department and the services very much had their ear to the ground about the things that were most compelling where people were asking for the most help, and we are already moving out on those things. That to me speaks to really good engagement across the department with the community both at the service-and-component level and down in software development teams. That was that was really exciting to see.

George: That takes a lot of work doing communication. It is so hard. Like Bill said, it is not technical. It is leadership and communication. The three of them are you have to fit all three together to do a transformation

Eileen: Absolutely.

Bill: My favorite quip from George Bernard Shaw is, *The greatest problem with communication is the illusion that it has happened.*

Eileen: That does speak to understanding how the data we use is effective to to different stakeholders about telling the story about achieving outcomes and achieving value or finding situations where we need to find additional support or additional investment. The data do tell the story.

On that note, I am going wrap this up. But I am going ask if each of you want to offer up any one final thought, question, or call to action for our listeners before we conclude today's podcast. I will start with you, George.

George: The challenge we have going forward is taking what we have done and turning it into action. We have got a good baseline. Things like the flow metrics. Getting the business metrics so we can actually look at them a little bit more carefully. Going beyond the like, the pipelines, the number and understanding at that business level. I think that is really the big challenge going forward. And then some of the the playbooks. We are just starting a study right now on working with some of the folks at SEI on organizational structure. What makes a DoD program different than a traditional program, and what is the right balance of resources in that program? Very practical business things as we do larger transformations when our program comes and says, *What do I need to look like to do modern development?* I think those very practical things are where we need to go next? We are done with the

one-year study. Let's just do a couple of like, *These are really focused kind of interesting questions.* There are so many interesting questions we can answer. We are going to start looking at the overall flow metrics and end to end and then looking at how we can help some of these legacy programs become more agile and more modern.

Eileen: Thank you. Bill, do you have some final thoughts?

Bill: My final thought is the DoD is an immense organization. As different as the DoD is from commercial industry, the DoD has so many that are really different from each other. So there going to be an awful lot of work trying to understand how to make this effective department wide.

Eileen: There is no shortage of good and interesting problems to solve.

Bill: Lots of interesting problems.

George: It is a fascinating place. Hopefully, people will actually go out and use the MEPCOM system. Join the department. We have good fun problems to go after.

Eileen: We do, and they are so important every day. One of the things I love about working here is you can always see the straight line to the mission. On that note, I want to thank you both for taking the time to sit down and talk with me today about this study. For all our listeners, I want to thank you for joining us today. We are going to include links in the transcript to all the resources that we talked about in this podcast.

The SEI podcast series is available in all the places wou regularly find your podcasts including Apple Podcasts, Soundcloud, Spotify, and the SEI's very own YouTube Channel. As always. If you have any questions, please don't hesitate to email us at info@sei.cmu.edu. Thank you so much.