Lauren Williams:

All right. Good morning.

Audience:

Good morning.

Lauren Williams:

Oh no, we're going to do that again. Good morning.

Audience:

Good morning.

Lauren Williams:

Thank you. I'm Lauren Williams. I'm Senior Editor with Defense One, and this morning I have the privilege of talking with David McKeown. He's the Deputy CIO for DoD and the SISO. David, thank you so much for being here.

David McKeown:

Yeah, thanks for having me.

Lauren Williams:

Before we get kicked off, I would like to save at least a few minutes for Q&A at the end. So if you have a question, definitely let me know and I'll prompt you for that. But we're going to kick this off. David, what's on your plate right now? What are your biggest projects, challenges? Tell us everything.

David McKeown:

Well, first of all, I want to thank everybody for being here today and this interest in this topic. The Department of Defense is vast, and securing it is very difficult. Top of mind is the recent unauthorized disclosure that occurred with the National Guardsmen. We've been working that hard, trying to accelerate some of the Zero Trust things that we want to put in place to get after that problem. We put out, within the CIO, some sort of reminders about things that people are supposed to be doing in the first place, like logging of accesses to files, downloads, and things of that nature. User activity monitoring, we had a big push back in the day to install user activity monitoring software on all of our classified networks, and we're just rechecking to make sure all of that is still in place, and that the rules are correct and would be able to detect anomalous behaviors that are going on in a workplace like excessive downloads, people going where they're not supposed to go and such.

And then, I'd say lastly, the key thing is least privilege implementation. Part of the problem in this scenario was the gentleman did have a proper clearance and did have access to the network, but just because you have access to the network doesn't necessarily mean you have a need to know the data that's out there. So we're working that hard too, to put some policies and procedures in place, some automation in place, to check people before they can get into those areas that they really don't have a need to know and get at documents. So that's top of mind.

Of course, we've been working on Zero Trust for quite some time now. We published in November our Zero Trust strategy and roadmap. It's got 91 capabilities to get to our target of Zero Trust. We set up a

Portfolio Management Office headed by Randy Resnick. He is leading the charge across the board and deploying Zero Trust across the DoD. He is working with a lot of teammates throughout the different services and agencies to get there. This year, each of them will have to come to Randy and show what their plan is to implement Zero Trust inside their service and agencies.

We gave them three options; one is to uplift your current environment with the right ingredients and integrate them together. Two is go to Commercial Cloud and have them provide a capability for you, so we've been partnering very heavily with Commercial Cloud providers, asking them to analyze their offerings, partner with other service providers to try to achieve those 91 capabilities to get us to target of Zero Trust. Really great relationships are forming there. As you know, we led the joint Warfighting Cloud Computing Contract, which is a IDIQ contract with Google, Amazon, Microsoft, and Oracle. All four of them receive contracts there. And that will be at the unclass level, the secret level, and the top secret level. And there are cross-domain solutions that'll allow data to flow back and forth between the classification levels.

So we're really excited about that and we're very strongly partnering on this Zero Trust initiative and that second coa that I was talking about with those Cloud service providers, so that perhaps we won't have to build much ourselves. Perhaps they can meet us with this great solution that we could just consume and operate out of a native Zero Trust environment.

And then, the last coa was we have been experimenting with how would we build an on-premises Cloud that was at the Zero Trust level. And for that one, we're targeting a more advanced level of Zero Trust with 152 different capabilities baked into that.

So all of that's going exceedingly well, lots of great partnerships going on with industry. I've been taking field trips with all the department SISOs to the Cloud service providers, to other industry providers that we rely on heavily, based on the pillars of Zero Trust. So for instance, we went to Cisco to look at what they're doing in the realm of the network pillar, and we have a lot of pillars to get through.

And then, we're also hosting a lot of vendors in the Pentagon, and we're structuring that in the same manner. We've got seven pillars that we're trying to satisfy here to get to the 91 capabilities. So we're having specific days, specific areas where the vendors can come in and talk about what they're doing for data, for user, for device, for network, for application, orchestration and automation, and then lastly, logging and analytics. So really good things happening there.

We're also focused on DIB cybersecurity. We continue to work on the CMMC rule. That's progressing pretty well inside the building. We're working through OGC right now to get that out of the building, get it over to the Office of Small Business, and then follow on to OMB. We're targeting late fall of next year where that can start to be put into contracts.

Hopefully you all are following that that has three tiers. At the very basic tier is data that is sort of important, but not important enough for us to go check your homework. You'll still have to do 801.71 proving that you can defend the data, but it'll be a checklist that you fill out and then you submit it in Spur, so it's a self-attestation.

At Level 2, that's where we start getting into CUI data, controlled unclassified information that we do care about. For those, we're going to have a third-party assessor, much like for FedRAMP, go in, perform an assessment on those vendors, and they'll get a certificate saying that they're certified to handle data at a Level 2.

And then lastly, for our golden nuggets, our most critical programs and technologies, Level 3, not only will we do that third-party assessment to ensure that they're at Level 2, but we're going to have the DIBCAC, which is a organization under DCMA, that will come in and do a really in-depth assessment of 801.72. And those are controls that are based on advanced persistent threats because the adversaries

that those companies are facing are first world cyber actors: China, Russia, Iran, North Korea. So we want to make sure that they're prepared to defend there. So DIB cybersecurity is a thing that we've been working on.

We've also been working on the innovation group out there, so small and medium-sized businesses working through pain points that they're having to be able to do business with the Department of Defense. Related to CMMC, for instance, what we're doing is we're going to be doing a pilot of a Commercial Cloud offering that is sort of automatic at Level 2 level. So instead of them having to prove that their home network or their company network is secure to handle Level 2 data, if they say, "We're going to go ahead and put this in Company X, which has already proven to be at Level 2, then we're going to give them full credit for that." And that kind of reduces the barrier to entry in doing business with the DoD.

But there are a lot of things in our engagements with the small and medium-sized companies out there that are responsible for innovation within the Department that they've highlighted from a security perspective, for instance, reciprocity and ATOs and all of those sorts of things. So we're tackling those things and engaging with industry on how we can streamline that and better do business with them.

And then, on the DIB cybersecurity front, just one last item, we are working on a strategy, a DIB cybersecurity strategy, that we hope to have out later this year. If you've done business with us, you know that there's a variety of folks within the DoD that provide a variety of different tools and assessments and things like that in support of the defense industrial base. For instance, we have DC3, the DCS program up there. They have a variety of free tools that we offer to industry for cybersecurity. We also have the Cybersecurity Collaboration Center at NSA. They share threat intelligence, and they also have some free tools like protective DNS and email security to offer to some of these businesses out there.

Our strategy is bringing all of the pieces and parts within the Department together and kind of laying it out who is going to be doing what. And we've overlaid everything on top of the NIST cybersecurity framework, so we will have the identify phase, what the government is going to do to help industry show that we can identify what needs to be protected. Then there's the protect, so what are the measures in place to protect the data? So CMMC would fall in that, for instance. And then, detection and response and recovery. We have things that we are doing to support industry in all of those things.

We will also be rationalizing the tools that we provide. For instance, the protective DNS is super simple to adopt, easy to implement. You don't have to be a rocket scientist at a small business to onboard to that. We want to field some tools like that that are a really good bang for the buck. They're cheap, they're easy. You don't have to be the greatest cybersecurity wizard in the world to implement them. And so, we're going to be rationalizing that list and putting that out too as to what we provide to everyone in a clear, concise way. Because right now there's a lot of different paths that people are interfacing with the Department and getting services from the Department. So I think I'll stop there. I think that was a lot.

Lauren Williams:

That was a lot.

David McKeown:

Yeah.

Lauren Williams:

You have a lot going on.

David McKeown:

Yeah.

Lauren Williams:

You don't even need me here. But starting with the strategy, when can we expect to see that? Is that something that's being worked on now?

David McKeown:

Yeah. I established an Executive Steering Group. I think we've been at it for about six months now. Congress, as a part of 1648, had asked us to develop a framework for DIB cybersecurity. So before CMMC came over to DoD CIO, last year, ANS took a couple of runs at going to Congress and having them sort of comprehend what our plan was. Every time Congress said, "Now this isn't integrated enough. It's not a single belly button. It's not clear to the customer out there." So I formed this group. We've been working at it for six months. As I said, we're dissecting it based on the NIST cybersecurity framework, great partnership amongst everybody in the Department that does things for the DIB. So I think we're getting close. We have fleshed out the actual line items in each of those areas, the identify, protect, detect, respond, recover. And I think we're about one meeting away from nailing all of those down. And then, we'll take that and then put it into words inside an actual document. So I think we're probably no more than six months away.

Lauren Williams:

Okay. I'll be looking for that.

David McKeown:

Yeah, absolutely.

Lauren Williams:

And then, asking more questions about it.

David McKeown:

Absolutely.

Lauren Williams:

But there's this theme, I think, with the Defense Department, especially as there's an increased use of commercial services and just leaning on the defense industry base writ large, and making sure that these companies that the Pentagon does business with, that they're secure. Because if they're not, then that means the Pentagon is vulnerable. Can you talk a bit about that sort of push and pull and what reticence, if anything, that you're feeling from some of these industry partners to become cyber compliant with things like CMMC?

David McKeown:

Yeah, absolutely. So on this particular topic, we're going to stay away from CMMC. These companies are going to go through much more rigorous assessments. So think FedRAMP, right?

Lauren Williams:

Mm-hmm.

David McKeown:

Think FedRAMP moderate, think FedRAMP high. And that's the starting point. So it will either consume something that has been assessed by FedRAMP, and I'm a voting member of the FedRAMP JAB, so I see the products that go through there. We look at the artifacts, we make sure that they're secure. So it's very rigorous. And then, once we in the Department decide we're going to adopt something, if there is no FedRAMP, we're still going to run through the FedRAMP process. But then, we have another set of controls on top of that that Roger Greenwell and DISA do the assessment on. It's probably 30 or 40 more controls on top of that to show that we like it, it's secure for the DoD.

We also create tenant security guides, how to lock down if you build a tenant in this Cloud, how do you lock that down properly? We build lots of guides for how to monitor and censor it so that it's just not sitting out there on its own, unprotected. So we do a lot of work there. And industry partners, Cloud service providers, they're in this together with us, right?

We did have an incident recently, and I'm not going to name vendors, but some of our data escaped. And I was heartwarmed by the sort of transparency and the desire to work together to resolve this, not only fix the problem that was encountered, fix it long-term so it will never happen again. And then, as a result of that, we are looking at our contract language and saying, "What should we modify?"

So in this particular instance, we said, "Not only modify it for that one company, but how do we do that for all the Cloud service providers that we do business with?" So if somebody's data inside our Cloud gets lost, let's say it's PII information, the company that it was their neglect and they lost it, they should have to pay for identity theft protection, right? That's one of the things.

One of the things we find, too, is we keep thinking of the Cloud service providers as the hypervisor piece of it, as sort of a one-time inspection, and then all we monitor is the client side. When we build a tenant out, we put monitoring in place, we're patching, we're making sure that everything is good on our side. But that Cloud service provider's hypervisor and management side, if that's broken into, all bets are off. They can do anything they want on our side.

So we're also looking at adding language about allowing us to red team constantly, whenever we need to, their side of the equation. Most of the Cloud service providers I've talked to have been totally on board with that. As a matter of fact, as a part of FedRAMP, they're supposed to do that annually on themselves. We're asking to see those results too when they do a red team, show us what's going on.

And then, we want to use some sort of outside-in scanning techniques like Xpanse, Shodan, to just kind of look at their IP space on their hypervisor, their management side, to see if doors and windows pop open that are unsecure. And then, we will help alert them and we'll help alert our own customers to the fact that a vulnerability has occurred due to some configuration change or some new device coming online that wasn't configured right in the first place.

So it's an evolution. So from that one event, because they didn't wall themselves off, they didn't lawyer up, we worked together, we came up with some things that we're going to make the whole environment stronger, and not only for that one Cloud service provider, but for all the ones that we deal with.

Lauren Williams:

And so red teaming, has that become more of the status quo, at least from the DoD side into these commercial services with the Cloud service providers?

David McKeown:

Well, red teams are a scarce resource. I would love for it to become the status quo.

Lauren Williams:

Okay.

David McKeown:

We have some other things that go on inside the Department that are very effective. We do a "Hack the Pentagon" and white hat hackers are allowed to look at stuff like that. So I think we'll explore more and more ways of getting after this. We don't have enough resources to continually red team everything under our purview, but we do want to intelligently deploy the red teams where we may have concerns. And initially, before we start using something, we want to make sure it's been red teamed and locked down. And then, the red teams, over time, we'll send them in where we need to to investigate things.

Lauren Williams:

Okay.

David McKeown:

And maybe something didn't happen, but we just want to go look, right? So it's important that we'd be able to do that. And most of them are welcoming that. That's how their own internal red teams work. And so, we're going to work through that.

Lauren Williams:

We talked a little bit about this offline, how time-consuming cyber defense is for the operators, the cyber defenders. Are you exploring automation? You've mentioned that a couple of times, but artificial intelligence, when can we expect to see more of that as the status quo for Pentagon cyber defense?

David McKeown:

Yeah. I don't think... We want to definitely get to a point where we're using AI. I talked about the pillars earlier. So in the area of logging and analytics, I think we can use AI to do that analytics piece better and learn from it. And then, under the orchestration and automation pillar, I think we could also then do some robotic process automation and say, "When you see something over here in the logs, then this is how you're supposed to respond automatically." Initially, we'll probably put a human in the loop and somebody has to say, "Yes. Go ahead and take that action." But there's a lot of things out there that I think we can definitely automate upfront. I don't necessarily think I want to have AI learning and doing without any humans in the loop.

Lauren Williams:

Yeah.

David McKeown:

But we can certainly use that to our benefit, and we can definitely use the automation to take action. If you've ever worked in a security operations center and see all the alerts that come up on a sim, it's overwhelming. And you've kind of got to know which ones are the most important ones to get after and when. So we can use all the help that we can get in automation. I think it will help us tremendously there.

And keep in mind, we're not really logging everything that we should right now. So when you increase the volume of all the data that's coming in, we really, really have to employ AI to get after that, because humans won't be able to keep up.

Lauren Williams:

So are you saying yes or no to ChatGPT in the Pentagon?

David McKeown:

I can't say yes or no. I know that our CDAO has expressed some concerns with generative AI, large data models, because the truthfulness of the data being shown, you can't really figure out where did that answer come from. It's not traceable back to the root of where the engine drew that information from. So that's concerning, so there's more work to be done there.

I think another sort of cybersecurity aspect that is concerning is some of those, whatever you all are typing in ChatGPT, it just consumes as part of the data set and then may spit out those exact things to someone else.

Lauren Williams:

Yeah.

David McKeown:

So in our building, if we're typing things about the F-35 that have some great details about the F-35 in a query, it becomes part of the gonculator and can become answers that somebody else receives, so that's of concern. But right now we don't have a policy on it yet. I think we need to probably hold a senior level meeting and figure out what that needs to look like going forward. But we're not using it for anything, so don't worry about that. We're not asking for what the next move with Ukraine is or anything like that.

Lauren Williams:

Yeah. No, for sure. So before I go to audience questions, I want to go back to the top of your comments. So Zero Trust, the goal is to have it fully implemented by 2027. Are you on track for that? And then, back to the intelligence leaks, do you think that it will prevent these leaks from happening in the future? Or how will having Zero Trust as the baseline change, I guess, the outcome?

David McKeown:

I feel very, very good about our chances of hitting 2027, just because of our partnership with industry in that second coa. And even on the third coa, they're partnering with us quite well to kind of build an ingredient set that we can deploy on our own bases if we need to in a tactical environment. So I definitely feel good about that.

And every step, every activity out of the 91 that we implement successfully makes us more secure. So even if we don't get to 100% across the board in every network and enclave and application out there, we're on a journey. And anything that you do to satisfy any of those things helps us become more and more secure over time. And many of the things we're already doing, so we'll take credit for those. But I think we're on a good path for 2027.

To your question about the unauthorized disclosure and Zero Trust, I think it will help tremendously while the data is resident on our computers. Okay? So we can restrict printing, we can do the fine grain access controls to the data. That will help. As I said, some of these repositories need to be locked down better and do a check not only that you have a security clearance, but you have a need to know that particular piece of data. So Zero Trust will definitely help in that realm. And if you look at what NSA did in response to Snowden, Congress said, "You need to fix this." They've implemented Zero Trust on their networks, and it works. So that, I think, is good as long as the data stays on the computers.

Now, if somebody prints it out and then walks out of the building with it, that becomes sort of a physical security problem. Or if the wrong people get clearances and get accesses to things that they're not supposed to, Zero Trust isn't going to solve that. I think the principle of Zero Trust, which is trust no one, always verify, applies, and least privilege. But it's a different realm than the cyber realm, in that case, once it leaves the computer and becomes a printed document or somebody takes a photo of it, of a screen that has that data up on it. It's changing mediums. And I can protect the medium that's on the computer and do that quite well, but as soon as somebody does those other things, it becomes somebody else's jurisdiction to deal with, so the physical security folks, the personnel security folks.

Lauren Williams:

Yeah. And that's its own separate challenge.

David McKeown:

Yeah. Right.

Lauren Williams:

We have two minutes left. Doing a check, does anyone have a question? Speak now. You have excellent access here.

David McKeown:

Sir.

Lauren Williams:

The mic is coming.

Andy Difazio:

Andy DiFazio. I work for Mandiant.

Lauren Williams:

I'm so sorry. Do you want to use this?

Andy Difazio:

Oh, sorry. Andy DiFazio. I work for Mandiant. You've been a visionary as it relates to security validation for the Department in engaging with a pilot program for security validation. How do you feel security validation applies to the developing Zero Trust foundational architecture?

David McKeown:

Yeah. Thanks for that question. I think security validation is very, very important. It almost, well, it does parallel the discussion of red teaming the Cloud service providers. Security validation is sort of a way for us to red team ourselves constantly, but do it in an automated way, and play pitch and catch with malware, use the same tactics, techniques, and procedures that the enemy would use. And it's all based off the MITRE attack framework. So the ability to sort of emulate that without actually having the red team humans sitting there doing it is very, very valuable. And it's something we want to put in place and leave in place to keep checking.

We built Zero Trust. We made sure it was there to begin with, but we all know that our baselines, our things change. People change settings on things. So we want to make sure that Zero Trust remains employed over time. So by playing pitch and catch with security validation and other red teaming tools, a very important concept for us, because we're not trusting that our baseline, that our security posture, hasn't changed. We're checking it constantly as well.

Lauren Williams:

David, this is great. And I could keep you up here all day because I have loads of questions, but thank you so much for being generous with your time and joining us today.

David McKeown:

Thank you. Thank you all.

Speaker 6:

Please welcome the Vice President of Mandiant-