Transcript for Session 3: Future of the Cybersecurity Workforce, Recent Trends, Workforce Demands & National Initiatives

Mary: OK, everybody, welcome back. Final session of the day, sadly, because it has been fast but fun , up is a terrific presentation, the future of the Cybersecurity workforce: Recent trends, workforce demands, and national initiatives. Our presenter is Dr. John Sands. Once again, post your questions in the chat window and make sure you click on "panelists and attendees, and we will do a little Q and day. -- a.

Dr. Sands: Welcome. Last session of the day, I hope I can keep your attention. We have some interesting things happening. When asked to do this session and thinking back on what is happening in this industry and what are the things that as a community involved, logistics, what are the things you need to be aware of? You are probably aware of some of these trends, but I want to go a little deeper and maybe give you a better understanding, and some resources that you could use in incorporating some of these trends and tools you will need to know about within your classes. That's my goal for this session so I will go ahead and share the screen. When I am asked recently to talk about, what is happening in industry that will be a significant change, that will have a massive impact, especially in your community, I really think what is happening with the CMMC program is the thing to be aware of. Hopefully have a better understanding of it. It stands for the Cybersecurity maturity model certification. So last year, what happened is that Congress funded a program in the Department of Defense supply chain, and I'm sure many of you are familiar with what's going on, and the idea is that in the future, contractors and subcontractors interested in applying for awards with any of the Department of Defense agencies or organizations are going to have to show that they have passed a Cybersecurity audit and they are moving along that path to maturity. This is all about a maturity model. Over the years, we've been training technicians and -- in Cybersecurity, how to use the different tools and how to assess different products and implement secure communications. There is a hold cap yacht of things. The framework -- there is a whole caveat of things. The whole framework spells it out. It says, these are things as an organizations you need to do, see what is applicable to your organization, and do them. The problem is, many organizations, just like people, will not necessarily do things unless they are forced and somebody is checking them. In many cases, they may not do it right. That maturity model is about bringing an organization like the

Department of Defense supply chain -- which, by the way, encompasses every aspect of business from uniforms to tools to jet airplanes. There is over 300,000 companies that this will impact. The idea is that the federal government is now embracing this idea of a maturity model and as a group, go through this process of maturing our cyber landscape and operational areas and institutions. That's what the CMMC is basically all about. About a year or so ago, two Cybersecurity centers got together, and I am from the CSSIA center outside Chicago. We work with many different institutions across the country in Cybersecurity. The insight center which is on the -- Ncyte center,, what do you know of the CMMC things? What if we put together a program and some content to distribute to the schools, specifically community colleges, that are preparing our future technical workforce? Maybe some classes to bring faculty up to speed and talk about how this information could be disseminated and integrated into curriculum. So basically, we took about six months and we did some pretty deep investigation of how we can do this and what the model encompassed and so on. And we came up with the course. Now we are in the process of going through the CMMC accreditation board to get recognized in their marketplace so we can use it throughout the marketplace. What the CMMC program is all about is to take this huge organization, Department of Defense supply chain, and make it more secure and resilient against cyber attacks. Let me give you a visual of what CMMC is all about so you can see visually. If I go here, this is a toolkit that was built at heartland science and technology group in Champaign Urbana and associated with the University of Illinois. These are tools in the future preparing for a cyber audit associated with getting there CMMC certification. What is CMMC? It builds upon this framework which identified 17 different domains, different areas that we need to be concerned about when we talk about Cybersecurity. It starts off with things like assess -- Access control, accounting, auditing and accountability, training, you get the idea. It goes across all these different ideas. They defined specific capabilities and organization needs to have in order to strengthen their organization against different types of breaches in cyber attacks and so on. But the idea is, you can't just throw this pretty sophisticated program out there for everyone to say, just do these things. What we need to do is build maturity, build the capabilities of doing these things and doing them right. But they did is they built a five tiered model and that is what the CMMC is all about, based on these 17 domains. Again, each domain will have capabilities and that's what we see in these item areas. You see what is highlighted in red versus pink and so long -- so on. There are five levels organizations can certify through, so everyone will have

to certify at Level 1. Level 1 consists of these specific capabilities. Then when we go to level two, transition every level, look how many we add on. It is a much bigger lift. Ultimately, we want to see all organizations get to level three so this is what Level 3 would look like. Then there is level four and level five covering all the capabilities. That is what the maturity model is all about, on boarding organizations to begin to not only think about and have a checklist of things they need to do as an organization to secure their systems and their information, but to prove it. How does that impact us as organizations that are training the next generation of code workers in this area? What we are trying to do as a center is create a course that I will share with you, and give schools the tools and resources to build into their existing curriculum and courses. I'm not saying this has to be its own standalone course or program, although I'm sure there will be schools that look into that. More often but I think we are going to see is, how can schools look at these things and build them into their existing programs? Can we create activities so that students learn, for example, if they are installing a firewall, it doesn't stop there. Yes, they need to know how to configure the firewall but they need to know how to test it and document to prove to someone that the organization's requirements and policies, that it has been tested and works. That might be logs or a series of tasks and so on, and collecting those artifacts and sharing them with a team preparing for an audit. So that's what this initiative is all about, and it really is the future of Cybersecurity, because I will guarantee you that the department of defense is not the only place that will do this. We will see more vertical markets and federal agencies do this. This is the future of Cybersecurity. We will not have -- not only have both practices and procedures spelled out, but we will want to have very specific audit items we look for to do business, literally to do business. You will not be able to get a contract with our organization without showing you have these capabilities. In a nutshell, that is what the CMMC program is all about. Just wanted to give you sort of a visual, make sure you've got the idea. Sure many of you have heard about CMMC and hopefully this takes out -- I've heard a lot of things like, it is an impossible thing, organizations aren't willing to do it, and so on. It is not an impossible thing because it was built as a maturity model, so organizations will gradually build to that level. Let's show you what a capability is. If I click on this first one, this is the actual capability. So up here, this is the first capability in the first domain. Establish system access requirements. So an organization has to prove that they can do this. What we are given out of the actual missed 171 framework, it gives examples and so on, and we will have tools where an organization will be able to

go in and be given information on how to collect the artifacts necessary to go through an audit like this. So, what we've done, again, the CSSIA center and Ncyte center have gotten together. They're having a workshop. We've offered, I believe five of these now, and they've all filled, so there is a waiting list. We've talked to people at the center here and we know there will be a need in this community as well as the Cybersecurity community. We are getting requests from all different areas of business that deal with federal agencies to have a better understanding of this, because this is really everyone's -- responsibility, not just the Cybersecurity people. Knees organizations have to have some understanding of this process and ultimately participate in the process of going through the audit. Let me show you what the course is all about coming to give you an idea. We put the course up in the canvas infrastructure in open website, so it is on the open website. We basically created modules that go through and give a pretty in-depth review of what CMMC is all about. To understand CMMC, you need to know about controlled, unclassified information. We talk about the use of a dashboard, chapter one basically goes and defines what the framework is all about and talks about the difference between -- talks about this advanced persistent threat which is the reason we have this. The old idea that's the whole idea of safeguarding federal contracting information, and then we go into the modeling. Some interesting things we've done with this course is we have built in interactive activities. We borrowed these from Brookdale community college. They had an NSF grant to create these interactions and we've built some of these for this course. I will show you and go into details with what we've done. This is the first chapter on what it goes through, and if you want to see one of the E-Mates, this is an example. It is written in HTML five. You can use this to do your lecture, or I can give this to a student, and many will have assessments that go at the end of them that we can measure their competency in the different areas we are presenting. Then it goes into the domains. But you get the idea, almost like a little e-book but it is an interface with the students, or you can use it in your presentations. We've embedded these throughout the course, so not only are in demonstrating what CMMC is all about and deconstructing the model and how it works, but when we get into the each of the domains dust into each of the domains, it will make sense as well. -- into each of the domains, it will make sense as well. We have a short interaction -- introduction to each of the domains. We've embedded them. We also have assessments throughout the course. And then, certainly a neat thing we have done as well is we've given interactive PowerPoint. Let me show you one of these so you can see this a little bit. And by the way, they are in the course itself,

so if you take the course, you will get all of these things, but if you go into files, and you go into PowerPoint, they are all up here. What we tried to do was make a PowerPoint that was more interactive and actually deconstructed the framework a little better than a typical PowerPoint. We gave these PowerPoint animations, so I will download one and show it to you real quick. Download it. And this is what it looks like. I want to share my own screen for a second. Can you see that? Is that working OK?

Mary: It is showing perfectly.

Dr. Sands: Here, we are basically going to the first domain. In the first domain, we are showing the first capability. And then, basically, the capabilities are supported by practices, and the practices are each of the five different levels of the model, so in this case, we have the first practice of Level 1 and other practices that level two and three. If you click on it, we will go in and look at the first practice. Limit system access to authorized users, processes acting on behalf of authorized users, and devices including other systems. We give some examples, and we show what's necessary if you are going through an audit. Here is what the audit would look for, the objectives. Here is acceptable evidence. We want to incorporate these things in our class to teach students how to collect this stuff. Finally, who might be interviewed as part of the audit? These would be the individuals that might be interviewed as part of the audit, and what types of questions might they be asked, and so on? It is very practical and this can be used in basically any environment. Also, what tests might be performed to prove that systems meet compliance? We basically do that for every practice, so we break this entire thing down and give you all of those things that would be necessary to go through an audit. You can extract these things and determine which might be useful in your courses. That's what the course basically is all about. Again, it is in campus, so the idea is once you go through the course, if you would like, you can actually get a copy of it. So you can download it and use it in your own campus and whichever system you are using. That is the CMMC course. Do you have audio? Do you want to talk about the enrollment part? Maybe not come OK. If you check chat, she's going to add the link to how you can register, but we've created a faculty development workshop for this community if you are interested in taking the course. We will be offering these starting in June and they are two day courses. You get all of this stuff with it. I didn't show you the full scope of the course. I just gave you a feel for it. I showed you the first chapter, and each of the other

chapters go into specific domains. It consists of 18 different modules, and each one of them have assessments and different activities and E-Mates and so on threaded throughout the program. That's all I wanted to show you with the course itself. And then I wanted to show a couple of the resources we are working on in the Cybersecurity realm with different national centers and projects. We have a couple of interesting projects that we might want to show you. One that I definitely want to take a minute and show you is that Mike and I -- Mike, do you have audio?

Mike: I'm on.

Dr. Sands: We've been working on a couple initiatives over the last couple of years, and one of the big initiatives in our community is reaching more down into the high schools and making high school students more aware of the opportunities and jobs in Cybersecurity. We thought about, how could we do this? Part of the problem we have is that most of these environments that Cybersecurity professionals work in, are not going to be real easy for people to get access to. There will be skips and so on, and most students, high school students will never have the opportunity to see these people working in one of these environments. We thought about, what if we bring the environments to the students themselves and do that through AVR experience? We actually were able to receive an NSA grant to do that. We are done with the first phase of it. I will bring up the devil on this, but the idea is what we are basically going to give to high schools and other schools and so on, is the ability for an individual to go through facility, a guided tour, you could say, through the facility, interact with avatars in that facility and environment, and be able to learn, who are the different people, what are the different job roles involved in Cybersecurity? What are the different knowledge and skills and qualifications necessary? This is what we came up with, the first iteration of it. It's got a little video with it. Is it on the right screen?

Mike: Yes.

Dr. Sands: It starts off by students checking in at the facility and getting their badge. So they come in and at the front desk they fill out forms and so on and get their badge. The idea is there will be avatars throughout this, and what we call Easter Eggs planted throughout the security that are throughout the talk about

qualifications, individuals who work there, titles. We get our badge and the person is off and they can go into one of seven facilities. Wise seven facilities? We base this again on the nice framework, broke it down into seven types of general work. We have a facility where we congregated avatars and do that kind of work in somewhat of a facility they would do it in. When they go into one, they will see tablets on the wall and they can click and get information about it. We will give them the nice things they get with a -- the things they get with a nice framework. The beauty is they can go in and access systems. There is music with it, I don't know if you are hearing the music. And they can open documents, interface with the avatars. We've tried to game affiant -- gamify it and make it more interesting than a PowerPoint. We had to put the information into a briefcase and use it to answer questions and finish a challenge when you are done. We can show videos in here. Am I sharing audio? Let me see if I'm sharing audio.

Mary: You are, but it's very low.

Dr. Sands: OK, this is the actual 3D map of the seven different areas, so they can teleport into each of the areas or take stairs or an elevator. These are functioning -- Mike: John, you are showing just your share screen. We are not seeing the video. We are seeing the Cybersecurity dashboard now.

Dr. Sands: I must have picked the wrong slide. Share.

Mike: I will share the link to the video and chat.

Dr. Sands: How about now?

Mike: Yep.

Dr. Sands: Here to open up a document, they could be watching a presentation and they can click on the different avatars and have discussions and find out information about the individuals that work in the facility. And again, it is a challenge --

>> A combination of technical know-how, persistence, and computer -- to be a specialist. They provide advice to users of software and other equipment in virtually every type of organization. There are two types of specialists.

Dr. Sands: You can even bring up an individual. I have an avatar that you can look at their credentials, inspiration, training, and so on. There are all sorts of things to interface with but it is more exciting for a high school student to explore this on their own, and we are trying to gamify this. That's the idea behind the 3D environment. Any student would be able to do this with just a simple Chromebook. So that's the next step with this. And then ultimately, Mike and I had this vision that we would use the same environment to do exercises, so a student goes through a series of labs and we want to test their capabilities, knowledge, and skills in a specific environment in a challenge, so we put them into a room that will require they use the skills they learned and have to react to different things around them. That is the next phase we see using this environment. The beauty of this -- and this is sort of Mike's idea -- that we can basically just change the skin of this. If we want to show health care, we change it into a hospital. If you want to show a manufacturing environment, we change it. You have similar avatars and Easter Eggs can be similar. You are just switching out the environment. So those are two that I wanted to share with you. And then I thought I'd let Mike talk a little bit about this project with E-Mates and what we've been doing in the area of Cybersecurity with E-Mates. it is at our website. Are you seeing this?

Mike: Yep, see it.

Dr. Sands: Mike has got a project for the National Science Foundation that he has funded, on the development of these E- Mates. I will let him talk about the background and what these are about.

Mike: OK, thanks, John. This is sort of an interesting intersection, because we were the project that developed the original introduction to the automated warehouse e-book, and built all those interactive's that went in that, so we worked on that and they just presented that for the supply chain center. So what we learned from that project was that the real value in those interactive e-books came from the interactive, so we proposed another project to build the interactive and focus on stem areas. The idea was that if we could just build interactive's to discuss the concepts students are struggling with. Everybody sieges -- teaches social engineering in Cybersecurity so is a great idea to do this. These are all HTML five so they work on any modern web browser. They will work

on a Chromebook, so it's very easy to distribute. They will even work off-line. Here, they are posted in a number of places. Some of them posted at CSSIA's website and some are posted at Nycyte. In Cybersecurity, we've built about 50 and have plans for about a number 30. If -- another 30. If you have an interest in a topic that you think would benefitNow we just added quantum computing and AI to our list. Again, the nice thing about this is that the student has to go and perform an action. This is baiting where someone leaves a flash drive that says payroll and you have to click it and plug it into your computer then your computer gets compromised. It forces the student to think about their role in getting attacked by social engineering. Here, you click on the cell phone and the Bad Guy is taking a picture of someone logging in. Again, I tell my students the bad guys always have red devil horns so you have to keep that in mind. It's a whole list of than the students can go through. Then they have a little bit of the fact that social engineering is on the rise. It gives them a nice overview of these. In the CMC course John mentioned, you look at the top of the Casio website -- cssia website, you have access control. That's a nice interactive that in addition to teaching from the CMM see, there's an interactive that you can walk students through and explain what an authorized access is, what authorized is. It go through the subjects and objects and what those are and how they access resources. I have used this a couple of times this week in my classes. One of the neat things is, you can explain all of this interactively. This one I like because when it's accessing the server, it switches to a subject then switches back to an object interacting with the user. Then you have I AAA which is interaction, authentication authorization and accountability. It's the process that we take an Cybersecurity in order to provide access to people. What else, we have biometrics on the list as something we like to do. We built a whole series of these. There are some in mathematics, some in electronics. At my college, we have some posted in chemistry, physics, and environment of science. I will put my email address here if anybody's interested. They can contact me.

John: You can see they are very interactive. There exercises where they are picking the terminology, they get the mechanics of it and so on. The idea is to really reach the different types of audience. There is audio, so it is very tactical, very visual. There is a significant library now of these and this group may be interested in some of the other ones. We have ones in and like electronics. If you are teaching -- I know we have simulators out there, but this is a really thing that runs in HTML five, it teaches basic binary then introduces the idea of algebra.

Were going to show a binary number that has a decimal. What happens? You turn the switch on, it adds one over two which is .5. We have .01, it's .25. When you put more than one of these, it adds them together so you would see with the actual number would be. If you are teaching the binary number system and you want to show basic counting, it will show you how you count and the students can take control of this selves and play with it to master the skill. It into do each of the different gates. This is my favorite that we have controllable gates that go along with the truth tables. If you put zero in, you get a one out. If you turn the switch on the light goes off and we get a zero out. The next one, two zeros in shows the truth table getting a zero out. We turn one on, it's still off. Which on the other on, it still off. Now we turn both of them on and the light is on and we see the logic within the truth tables. We did this with each one of them.

Mike: I used this this week to teach exclusive or to my students.

John: Again, these are free tools and it's not just Cybersecurity, there are things like mathematics, electronics, other areas we are bringing them multi-disciplinary skills where they can use these tools. That is the second part of what we wanted to show you. Again, I put the link in the chat so if you're interested in using these things, you can use them online as it is or if you contact us, we can tell you how to download them. The beauty is they will run on anything. That will run on a smartphone. They will run on a Google Chrome pad. We are running and IOT collaboration. By the way, there are sums on -- some on meters, latches, simulation so want. Also, quite a few on networking there is one on teaching seven netting as well. -- sub netting. It shows that it is controlled by using this method -- mask and borrowing bits. Here, we are borrowing the bits and what it looks like in the mask itself and how many subnets it creates. Then, we add to that by how many users are in each subnet. We dragged this across. It's great to lecture with this, but it's great to give your students later so they can master the skill. Then, there's practice throughout. It tells them immediately if they got things wrong and they can fix them.

Mike: I found once students go through this on their own and their comfortable with the answers, they have mastered sub netting.

John: It's very visual will make it to the networks themselves. We show what a network address is, a usable address. Now we have two network at work --

addresses. Here's the summary of each one. We go through and keep seven netting this. -- SUBNETTING this. Then, we start introduce them idea of a magic number and a multiplier. The beauty of this at the end, we test them. We have this network subnet into parts and they have to give us what the addresses would be. The next one, were going to ask the usable addresses. It's a different way to teach this. More interactive and a it is been very effective. -- more interactive and I think it has been very effective. The last section they talked about, we did a couple of exercises. What we are doing is teaching how to do basic electricity and electronics. This is just a project where they are creating an intersection of North and South East West intersection. Here the green lights, yellow and red. We are using a board to basically program these and the beauty is taking learn how to code these as well. You can go in and see the code itself or both. We can actually run it. If we basically say simulate, it will start to run. Green lights in one direction, red light on the other. You get a yellow light, then they switch. We can teach basic processes and so on. In one of the books we did, it incorporates electronics and a whole bunch of different processes that would occur in a factory. These are examples that you can use in the classroom with phase. The last thing, Mike is come up with a great idea of testing someone with an escape route. -- escape room. He is going to teach some of those concepts and students have to prove their mastery to get out of the room. This is HTML five. It's easy to port onto any form and students that I have had use these really love it. It really brings students to a whole other level of engagement and teaching them self in many cases. We showed this to a high school student, we demonstrated this and didn't teach them how to use it at all and they figured it out then the next show, they described how to use the entire environment, how they solved each of the things. This is with the power of these things are. I will pass it to Mike this point.

Mike: We created two versions for a midterm and two for a final. This is for an ethical hacking course. The way it is set up, hopefully the sound works. You get a little scenario, you enter the room and the chandelier falls and the lights go out and you have to look around in the dark and clicked for the lamp to turn on. Then, you see that you have your resources to. -- your resources to. Then you have a checklist. You have defined these answers in order to be able to get out of the escape room. They are basically moving around. Whenever they find something, they can click on it. The piece of paper with a lighter, they turn on the lighter and it basically shows them of their is a password and it looks like it could be a username. That gets added to your resources. They are moving around looking for

any items that are clickable. This laptop, you can log in so you can try the username and password to see if it gets you anything. Here you have some of these doors can be opened. There might be some books you can click on. This one looks like a tablet and it has a login for the tablet. We have answers also, so if you want the answers we can share the solutions with you. We are working on an unstructured -- instructor guide for these. I talked to high school teachers who use this to reinforce things they have already taught, but then use it live with students were to go through. This is an old-school iPod so if you're old enough, you remember these. If you click on this, you click the play button it's going to play Morse code. For later in the challenge for that iPad, you may need to know what that is. Now, students have to go out or if their faculty if they are old ham radio faculty, they might have to brush up on their Morse code and figure out what that messages. Just work their way around find anything they can that they can click on. Over here, they click on remote control and it puts on a capture on a screen over there. They work their way around, they click they had to explore, but they are trying to find anything they can that will give them information that will help them fill out the list of that report checklist. There are other drawers as well. This was really the inspiration for the 3D. This is another drawer. Something should be clickable. As I said, the final exams are different rooms that have different objects in them, but they have the same learning outcomes. Same thing for the midterm, different objects and their but the same learning outcomes. It forces a student to engage in this environment rather than taking a standard midterm exam that they would normally do. That is just one example of what we built.

John: I think we have come to the end. Are there any questions?

Mike: Those escape rooms where the inspiration for what we did with the virtual reality environment.

Mary: Thank you to you both. Thank you for an interesting presentation and so many resources, so much the forecastle be able to use. I have a couple of questions that came in. In terms of the supply chain faculty, the teachers, what are the most important trends in Cybersecurity that they feel they need to prepare their students for?

John: I will take that on. I would say that Cybersecurity has come to a point that it is everyone's responsibility. It doesn't matter if you are an electronics technician, industrial controls person, if you are the person ordering or installing equipment things like that, it is everyone's responsibility and everyone has a part in keeping the environment safe for in some cases, allowing for someone to take advantage of that space or penetrate that space. Unknowingly in many cases. That is why it is absolute critical and I think everyone in the organization needs to be aware of what is happening. The other thing is how IOT and the proliferation of smart devices, cloud-based intelligence all these things are changing the way we do things every day. You may not think that your information is out there, but you would be surprised at how much information is publicly available to an individual who wants to do harm or a nationstate or a foreign actor or whatever it might be.

Mike: I would add to that, in then environment, you are running devices or appliances that may not be easily updatable. If there is an upgrade or update available to a firmware or operating system to equipment or instrumentation, you want to get that because most of the time those updates have security fixes and patches so you want to make sure you are running the latest and greatest. Don't assume that your devices are secure out-of-the-box. You want to be very proactive about making sure that they are secure and also a lot of organizations now they take some of their devices and the airgap them meaning that they separate them from the production network and they assume that they are protected then I don't have to worry about the security of those devices because nobody can get to them. Attackers have figured out how to jump the airgap and get to those devices. You even have to consider the security of those devices that you think might be isolated.

Mary: There's a whole lot of things that are going to be pertinent now and going forward for these educators. One last time for we close off, I want to go back to the faculty how our attendees can enroll in those workshops. Give us one more plug for those, because I think that is an exciting opportunity.

John: I will put it in the chat. This is the actual link. We are in the process of scheduling some Neil Gorsuch in June. -- some new courses in June. If you would like a specific course for your group, we have funding for this. It's just a matter of logistics. I think that course would probably be better -- very beneficial to people in this community.

Mike: Here is the center as well if you want to join and become a member. They have the links to any new training they are going to have, any upcoming training so you want to follow this website and make sure you stay aware of what they are doing and providing. If your school is looking at providing a center of academic excellence, this would be your first point of contact as well because they provide mentoring for that process.

Mary: For me personally, learning how widespread the requirements for the certification and how it's going to grow, to me that was like a call. Above and beyond all the security it's just going to be required. There's no getting around. Thank you both so much for your presentation and for making these resources available to this community. I think that is great. With that, we're going to welcome back Val for some closing comments.