ICT Educator Webinar Series

California Cybersecurity Career Education Pipeline and Pathway Project

September 11, 2020

Table of Contents

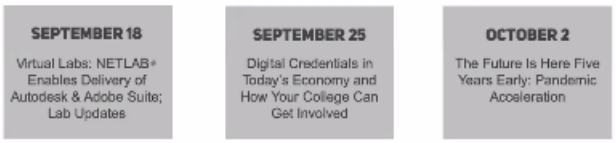
[00:00:00]

Welcome

STEVE WRIGHT: Good morning, everybody, and welcome to the ICT Educator Webinar Series for the fall of 2020. I'm Steve Wright, the Statewide Director for the California Community College ICT Sector Team.

If you visit our website, you can see our ten Regional Directors and Nicole Sherman, who is the producer of this series and our newsletter. Also, on our website, you can find various pathways material and other prior webinars that we've had over the past year. We've categorized them for you now, so they're easy to find.

Of course, everything we have on our website has been video edited, recorded, chapterized, transcribed, with the original PowerPoint presentations for your later use. A lot of people find it very helpful. We've had 3,000 views to date, and our archive is a valuable resource for faculty.



Coming up in the next few weeks after today's webinar, we're going to have a look at Virtual Labs next week with NETLAB and some of the auxiliary testing in lab environments that can be had with that, which is particularly relevant in this COVID period. Following that, Digital Credentials—we'll be talking to Peter Janzow again, VP of Credly. He's going to give us an update on how those are going educationally, educational technology throughout the world.

And we'll hear from Peter Coffee a futurist from Salesforce, who will talk to us about… We asked him, "What can you tell us about the future, now that we've got COVID?" He says, "Well, the future is five years early," so I'm looking forward to his perspective on that.

[00:01:31]

Today's Agenda

STEVE WRIGHT: Today, we're going to hear about a template for cybersecurity pathways, competitions, work experience, that can be used across educational systems and employers in California. Here at the community colleges, we have about 80,000 students in IT-related courses at any one time, with about a 75% replacement or turnover rate, so we're very interested in how to capture more of that potential into the cybersecurity industry.

The lightning rod or champion of this effort so far has been Dr. Keith Clement, and he's going to be our featured speaker telling us about the statewide taskforce and that sort of work.

But going on in the background for quite a number of years has been the efforts by Dr. Markus Geissler and Richard Grotegut to put together a California Community College IT Model Curriculum updated, all CID'd and with plenty of rigor and everything, updated now for cybersecurity. So, they'll be talking about that as well.

OK, Keith, take it away.

[00:02:32]

What Educators Need to Know about the California Cybersecurity Career Education Pipeline and Pathway Project

Prepared by Dr. Keith Clement

- Professor, California State University, Fresno
- Chair, California Cybersecurity Task Force,
  Workforce Development and Education Subcommittee
- Chair, California Interagency Advisory Committee on Apprenticeship (IACA),
  IT Subcommittee
- Chair, Public Safety Education Advisory Committee (PSEAC)
  of the California Community Colleges

KEITH CLEMENT: So, my name is Keith Clement, and I am a Professor of Criminology at California State University Fresno, and on the side, what I've been doing is I chair the Workforce Development and Education Subcommittee of the California Cybersecurity Task Force, Workforce Development and Education Subcommittee. And related to that as well, I do a lot of stuff with the California Interagency Advisory Committee on Apprenticeship (IACA), and I chair their IT Subcommittee.

For those that are not familiar with IACA, they are the state entity that is responsible for the development and design of new and upcoming apprentice opportunities like you would frequently find in IT and cyber.

And lastly, I had the honor and the privilege of serving as the Chair of the Public Safety Education Advisory Committee of the California Community Colleges, so I'm very familiar with, and have been working closely with, California Community Colleges for years and deeply appreciate, Steve, your invitation, and would like to recognize many of your Cal Community College colleagues for their spectacular work in this area, like Markus Geissler, of course, Richard Grotegut, Olivia

Herriford, for example, Tobi West, our friend Steve Linthicum, who recently retired, Nancy Jones, of course, and many, many others. I couldn't go into all of them, of course.

[00:04:07]

California Cybersecurity Task Force, Workforce Development and Education Subcommittee

- The California Cybersecurity Task Force (CCTF) is Co-Chaired by the California Governor's Office of Emergency Services (Cal OES) and California Department of Technology (CDT).
- The CCTF is made up of several Subcommittees like Information Sharing, Critical Infrastructure Protection, and Risk Mitigation.
- Facilitates collaboration, engagement, and partnership with cybersecurity and IT Industry (Employers), the Public Sector, and Education/Higher Ed.
- Works with California Department of Education, California Community Colleges, California State Universities, and University of California on cybersecurity education and workforce development programs.
- Wrote 2 key California Cybersecurity Education/Workforce Development Strategies (discussed in the following slides)

KEITH CLEMENT: So, in any case, the Cybersecurity Education Subcommittee is co-chaired by the California Department of Technology and the California Governor's Office of Emergency Services, and this is an advisory board to senior California administration on these types of matters of cybersecurity and emergency management, homeland security, etc.

So, when talking about the CCTF, we have a variety of subcommittees, and Workforce Development and Education is one of them. Our purpose, of course, is to facilitate collaboration and engagement and partnership with cybersecurity and IT. And by industry, we don't only meet employers of the private sector but also public sector employers as well, mentioned next—working with government agencies and organizations.

And what's really key, Steve, I think, is the development in tandem of IT and cybersecurity education and Workforce Development programs, in combination between education and higher education. So, we really are talking about reaching students as early as possible. Now, of course,

in California, it used to be ROP (Regional Occupational Program). Now it's called CTE (Career Technical Education).

Career Technical Education begins in the seventh grade, generally speaking. However, many of us in the tech and the IT/cyber area understand that we need to be starting these things as early as possible, and if we wait until seventh grade to begin, a lot of this… We're in trouble there. So, we have a strategy that directs there. We, of course, work in combination with the education institutions that you wrote, right there.

And what I want to spend a bit of my time on is talking about two key California Cybersecurity Education/Workforce Development Strategies that we'll be talking about briefly here. That's what I would like to talk about. And it's my understanding that if you have not yet received a copy of that somehow, that Steve, that maybe this would be available on the site for their view, etc.

[00:06:39]

California Cybersecurity Workforce Development and Education Strategy and Framework

- *The California Cybersecurity Workforce Development and Education Strategy and Framework* was released this week.
- The Strategy develops a framework through 15 recommendations to implement a cybersecurity **career education pipeline and pathway** to prepare 50,000 entry-level entry level professionals in California between 2020-2030.
- Some students (the top talent model) will complete STEM two-year/four-year degrees. Other students go into embedded stackable certificate programs linked with an 2000 hour On the Job Training (OJT) workforce development opportunities.

KEITH CLEMENT: So, the first and the larger document—about 75,000 words, so it puts it in the thick novel category, 273 pages total. It was supposed to be 210, so there you go…

The strategy develops a series of 15 recommendations to develop a career education pipeline to prepare 50,000 entry-level professionals in California between 2020 and 2030. We were on a call yesterday from a fellow from the national organization at this level. He says that the

entire U.S. currently graduates 15,000 cyber professionals in terms of degree programs a year. That's national. So, in any case…

What I want to emphasize is the idea that we have a model that addresses all components of talent, right? We have people that want to be the CTO or the CCO of Boeing or of Walmart or Amazon, and we have folks that are just happy to get their foot into the door and get a job that makes good money and supports their family, and everything in between. Everything in between.

So, with that in mind, we have to have this talent model that has two-year/four-year degree components. And one of those, of course, is a STEM-based degree program—heavy math, heavy science, all that kind of stuff—all the way down to what many folks are going to need or meet minimum job requirements for—embeddable, stackable certificate programs that are offered through the Cal Community Colleges, through the CSUs or the UCs, theoretically speaking, private universities. I want to certainly acknowledge private universities. I know the value of our friends over at National University and USC and Stanford and our other large private institutions.

But embeddable, stackable certificate programs linked with 2,000-hour on-the-job training, apprenticeship workforce development-based opportunities. So, that would be the 2,000 hours, of course, is the equivalent of one year of full-time work, and that would be added on top of the education programs.

So, how do we do this? That really is the question, is 'how do we get this done?'

So, through these 15 recommendations (some directed at K-12 education, some directed at the two-year and the four-year and the graduate programs)… And the industry-recognized professional certifications. Through coordination and collaboration, we are able to develop a pipeline that is what we call 'vertically aligned.'

So, each program shakes hands with the education program that came before it, and then shakes hands with the programs that come after it. So, we're talking about middle school to high-school transition, high school to two-year school transition, two-year to four-year school transition, four-year transition to six-year. And I also want to say that that's the college

preparedness track. We also have a career readiness track as well for those that don't need a four-year degree and a bunch of apprenticeship hours to get to what they're looking to do.

[00:10:22]

California Cybersecurity Career Education Pipelines and Pathways Include

- K-12 Education-- Career Technical Education (CTE) Industry Recognized Certification Programs; "A-G" Curriculum Integration (students meet academic and career education requirements); Dual enrollment, etc.
- 2 Year Associate Degree Programs and Certificates-
    - California Community Colleges
- 4 Year Degree Programs and Certificates-
    - California State University
    - University of California
- Professional Certifications and Training-

KEITH CLEMENT: So, this career education pipeline and pathway includes these various components… I don't really want to get into too much as we go down the list because you are the professionals in this field, and you are the experts in this area, so I don't need to talk about some of that.

But I do want to talk about the development at K-12 of industry-recognized certification programs. So, if you have a chance to go see the California cybersecurity essential workforce youth, pre- and registered apprenticeship talent model… That is a lot of words, as it turns out. For those that want to see how this aligns from fifth grade all the way to a four-year degree, you would want to read this part of that report.

But what is key is that we are getting kids into certificate and other types of programs as early as possible. And for example, in my ideal curriculum—and I put it all out there… So, in the ideal world, a lot of these kids are actually getting their first certificate out of the way in middle school. And is it an advanced certificate? Well, obviously not, but it is getting them ready to get them started to get through.

And actually, a second key component here—many of our IT and cyber students are short changed, in a way. That is that they are unable to double-count courses for both the academic side and the career preparation side as well. So, it's called 'A-G' Curriculum Integration, where we're literally developing high school classes that meet a graduation requirement, as well as a career tech requirement. And obviously, when they get three career tech CTE courses combined in a certificate program, high school students would be graduating with, cybersecurity or IT or related technical fields, certificates in those areas.

And that is listed, of course, in great detail at the large statewide strategy report, as well as the essential workforce report that I just mentioned.

This has already been done for history, government, math, and I did a physics course with Tony Coulson from CSU San Bernardino that many of you probably know in this space, and I think that he did the history and government of cybersecurity, and I did the Physics of Hacking course. Details are details.

Also, a need to have dual enrollment courses—that is another way that our students in our collective fields are not meeting the full advantage of the educational system, where they are basically taking high school courses that count for college credit. And I could have sworn I heard yesterday—Steve, correct me if I'm wrong… I heard somebody from a school district down south, Moreno Valley, who said they had at least one student in the recent spring that simultaneously graduated high school and community college through dual enrollment. I don't know if maybe I had a Zoom error and I heard that wrong, but that's what I heard the other day, so…

Two-year associate programs—

STEVE WRIGHT: Donna would know about that. I'm sure she'll share it in the chat.

KEITH CLEMENT: Oh, perfect, perfect.

AUDIENCE MEMBER: Yeah, we have a dual enrollment high school program at Moreno Valley. I'm from Moreno Valley, and we have a lot of students who get their AA degree and their high school diploma at the same time.

KEITH CLEMENT: Fantastic! Fantastic! That's the kind of thing that we would like to see on a statewide basis. We would love to see the Moreno Valley school district's innovation in this area pushed out to every district around so that we can get all access, right? All students should have access to these programs, available to these programs, you know? I'll talk about diversity and inclusion—everybody needs to have access to these programs.

So, in any case, I don't want to talk much about the two-year and the four-year stuff because I know that Markus and Richard are going to have a lot to say about that, and I don't want to talk about anything that they would get into.

But also, the linkage to professional certifications and training, right? So, we really are talking about 'how do we do a better job of blending academic education programs with the professional skill-based work experience types of opportunities that students in this space need?' I mean, I like to use the example of you can read all about a firewall in a great textbook, but until you actually have done it yourself, it's still theory.

[00:15:31]

The California Cybersecurity Essential Workforce Pre- and Registered Apprenticeship Talent Pipeline

- As a supplement and appendix to the previously mentioned strategy document is this pipeline with the following components:
- Describes the obstacles, limitations, and challenges faced by the education community/industry/public sectors in Cyber workforce.
- Provides a vigorous case for apprenticeships to help solve the cyber workforce capability and skill crisis in California.

- This model includes the following phases: 1. Recruiting Phase, 2. Pre-Apprentice Phase, 3.Registered Apprenticeship Phase, 4. OTJ Phase, 5. Prepared Workforce Phase! ☺

- Initial 2 Certs: Cybersec for Small/Medium Business & Life Sciences

KEITH CLEMENT: I spoke about the essential workforce talent pipeline. I had already mentioned it. It's a supplement to the previous larger statewide report that directs and guides us on the development of a pathway and pipeline in this area, but this report is actually interesting because it starts off with an analysis of the obstacles, limitations, and barriers that our education institutions have to deal with in terms of IT and cybersecurity education programs—like, for example…

And I don't want to get into any details here—it's become increasingly clear that many of our college administration folks do not necessarily fully understand what we're trying to do around here. They don't understand not only the value of it but what a program actually looks like. So, I have a lot of college administrators that don't want to have a cyber program or information security or IT program because they don't want to set up and maintain the networks and sandboxes and the cyber ranges that they would need to give the students the exact hands-on skills that we just talked about them totally having to have! In any case, that's an example of a barrier, an obstacle.

But not only understanding the barriers of the education community but also of industry, right? I mean, industry, for example, needs to work on collaboration with educational partners so that we can do a better job of understanding the current minimum and preferred requirements that they have for jobs that they're looking for right now.

And I don't just mean a one-time meeting of the minds, so to speak. It is clear that this meeting has to be a regular event—annual at the least, maybe every six months—to make sure that industry is able to effectively and strategically communicate to our education and our government partners exactly what it is they seek for workforce.

And actually, I think an easy way to break this down is on the basis of specific occupations—specific IT or cyber occupations—that actually correspond to an O*NET code that we can thus

analyze. For example, Cyber Analyst or Cybersecurity Engineer or Cyber Technician—those are example bellwether benchmarks of occupations that we really want to keep a thorough idea and close contact with what they are actually looking for, on a regular basis.

So, I do this for industry and public sector… A vigorous case for apprenticeship. An apprenticeship is a vocational model that is underutilized in what we used to call 'white-collar' positions. We don't call them necessarily white-collar jobs anymore. We've begun to call them 'new-collar' jobs. So, new-collar jobs are blue-collar in a sense, they are white-collar professional in a sense, and they are management in a sense, simultaneously across industries, across occupations, across sectors, which is one of the reasons why we have difficulty in forming the educational workforce pathway that's of benefit.

So, let's see… Model includes recruitment phase. The recruitment phase—in order to recruit diverse and inclusive groups, we need to make sure that, when we do the recruiting for IT and cybersecurity education and workforce development programs, we actually do it at the community level—not the state level, right? We're doing it at the state level. We're doing it at the regional level. We're doing it at the local level. I'm talking about doing it at the community level, and I mean the neighborhood level.

That's what I mean by recruiting and outreach, and that we are recruiting from all neighborhoods, and we are going to seek a diverse and inclusive workforce by going into a neighborhood-by-neighborhood basis, showing students and their families what they need to do to be successful in these programs through what we call Cybersecurity Education and Workforce Development Roadmaps.

These Roadmaps lay out the education and the workforce and how they make the combination, what programs are being offered at what schools, and what positions are being opened and where they are, all these kinds of things.

We have a pre-apprenticeship phase, a registered apprenticeship phase, an on-the-job experience phase (the 2,000 hours aforementioned), and a prepared workforce phase—and look, even a little smiley face, and I guess that would be phase six.

Because of COVID-19 pandemic response, we are working on an emergency basis on at least two certifications right now. The first is to support our small- and medium-sized businesses, and the second is life science, but I want to include in terms of life science to be health and medical as well. Those are two industry sectors that are being very hard hit by COVID-19, like many of our industry sectors. Economy and workforce have been done.

[00:21:09]

Key Discussion Points

- How do we engage with 90-100k students in IT-Networking-Cyber?
- How can we figure out a process by which students easily transfer/transition seamlessly across all levels of education state-wide in cybersecurity (and related fields?)
- How do we align and link K-12, 2-year, and 4-year education programs (degrees and certificates)?
- Accelerate CCC IT-Cybersecurity Transfer to 4 year education institutions.
- Credit for prior learning for completion of industry certifications.
- Other points for discussion?

KEITH CLEMENT: Key discussion points… How do we engage with the approximately 90,000 to 100,000 students in IT, Networking, and Cyber in California Community Colleges? And how do we make sure that all of those students have an open and available talent model that allows them to get to where they want to be in life?

I think that another key discussion point is 'what is a process by which we can utilize so that students can transfer and transition seamlessly from one education level to the next?' Again, middle school to high school, high school to two-year school, two-year school to four, four-year to graduate programs.

And I mean this on a statewide basis. There are plenty of lovely examples… Plenty of lovely examples of a school here or a district here doing wonderful things, and what we need to do is find a way to transfer the knowledge and innovation of our digital leaders in this area to other parts of the state that do not have the same programs. This really is a statewide effort. We don't want to recreate the wheel. We want to make sure that best practices are circulated widely and the resources are available so that other schools, districts, campuses, everybody and their students can be better served.

How do we align and link the K-12, two-year, and four-year education programs, again, to serve all aspects of our talent model?

We want to accelerate. Again, the Cal Community Colleges have had an IT model curriculum. They have had a computer science AST for quite some time. We're talking here about how can we work on the four-year school side to provide additional opportunities for all of those students across the tech field—IT/IS, software development, computer engineering. There are plenty of involved disciplines here.

We really need to have a credit for prior learning discussion. Many of the key minimum preferred requirements are found on the basis often of professional certifications, of which students are taking professional certification-like courses on our campuses. And we need to find ways so that they are acknowledged and provided support for their industry certifications in an academic sense. So, credit for prior learning…

There are, of course, other points, like transfer and matriculation and degree program stuff. Those are details for later, of course.

Like to see a copy of either Strategy Report?

Care to join the California Cybersecurity Education Workgroup?

Please Contact: Dr. Keith Clement, Professor, Fresno State University

Chair, California Cybersecurity Taskforce, Workforce Development and Education Subcommittee

kclement@mail.fresnostate.edu

[00:23:58]

Questions or Comments

KEITH CLEMENT: Questions or comments, and if you would like to see either report or have interest in joining the Cybersecurity Education Workgroup, here I am. I'm pretty to find, as it turns out. There's my email. And I don't know where I am for time.

STEVE WRIGHT: You're doing well. You're doing very well, Keith. I think before we transition to Markus and Richard, your presentation brings up a lot of points, and you talk openly about what we need to do and that sort of thing.

I think when we look at this, we have to ask ourselves, "Where's the leadership coming from? What is legislative mandate? What is the governor's office thinking?" Because a lot of us have had these ideas off and on for many years. We've seen the technological change, the revolution. But then, when we go to try to change the architecture of how things work, it's a brick wall. So, how do you perceive this going forward? I mean, a lot of good ideas are in this room right now, but how do you perceive us breaking through the wall?

KEITH CLEMENT: Well, Steve, that really is the million-dollar question, right? I mean, we can have the best curriculum. We can have the most rigorous statewide cyber competition league at all levels—semifinals and quarters… You know, a Governors California Golden Cup for the winner. There are a lot of those things we can do. But yes, let's talk about commitment.

So, I don't know, for those that were able to join us on September 2nd at the California cybersecurity industry convening, one of the issues that we thought essential is to make sure everybody on the call and paying attention to these matters was perfectly aware of the position of many key leaders in the state of California on this matter. I would argue that if Governor Gavin Newsom has his Secretary of Labor and Workforce Development and Director of California Office of Emergency Services, cybersecurity and Homeland Security Advisor to the governor, and he, last minute, had to leave, as you may recall… It is a difficult job being the Director of Emergency Services for the state of California these days. So, who steps in on his behalf? We thank so much California Department of Technology Director/State Information Officer Amy Tong. We also had Governor Gavin Newsom's Small Business Advisor councilor to Governor's Office of Business Development as well on the… You know, assistant secretaries of esteemed California state agencies. We had all the right folks from industry, including IBM, Amazon, right? Big firms.

And let's be honest—the reason why we wanted this convening to happen was to give everybody a sign of exactly how serious we are in the state of California on cybersecurity/IT workforce development education. I think 2020 is our year. Those two reports to be read and consumed at will—these programs exist. More are coming online. I think that the support is there.

I'm thinking about the only way that I personally would like to see more support is on the budget and the financial resources department, but let's be honest—with a $55 billion deficit and whatever is going to happen to education in the next couple years in this state, probably not the time to be asking for a $25 million or $30 million infusion to do anything brand new. That might just mean my budget analysis, but there you are…

STEVE WRIGHT: Well, it just means we've just got to make a good case for it.

KEITH CLEMENT: Yes.

STEVE WRIGHT: That's great. And you're certainly, as we said before, the lightning rod. You're the champion. A lot of these moving parts and pieces have been around the state for a long time, but

until you got involved, we didn't have a common place to go, and you're bringing that together, and I want to thank you, for everybody here, for the work that you're doing in leading this effort.

KEITH CLEMENT: Deeply appreciated. And I want to give a shoutout to you and your California Community College colleagues that have been carrying the ball for the last couple of decades in this area. And actually, I do believe that Markus and Richard and Olivia actually wrote the introduction to the two-year program component of that strategy report aforementioned. It talks about all that kind of stuff right there. So, I mean, it's in writing, not just…

STEVE WRIGHT: I love it. We're going to turn it over to Markus, I believe, for his presentation in just a second. So, Markus, you might want to get ready.

But the thing that is unique about the situation—and I guess I love it, because technology has exploded in all these areas, and academia hasn't really been bad. It hasn't been wrong. It's just totally unprepared for things to move this quick. And what started off as kind of a tech job for someone with a toolbelt has suddenly become a professional endeavor—and how do we deal with that? So, it's a wonderful, wonderful challenge.

All right, now with that, what we do know is that over the past… I've forgotten how many years, Olivia, you and Markus and Richard have been looking at this kind of stuff, but a model curriculum emerged, an IT model curriculum initially, and it's been adapted to cyber, and I believe you've even got adaptations to cloud. And it's a core curriculum. It's very fundamental in a lot of our community colleges. We have a number of students taking these courses. From these courses, they can get certificates and industry certifications and that sort of thing very easily.

We find it's interesting these days that a lot of the rigor that we have in these courses is greater than the rigor that you might find in more popular-sounding alternatives, like the Google IT certificate or whatever. And we know that people are pulled by names and brands, and that's very important, but I think it's the competency of the California Community College system. I believe that were sixty-something Cisco Academies and the number of students and the whole NETLAB and other virtual lab expenditures that we made… We have a lot…

Richard, you brought up the point the other day—the number of people who are professionals already working who come back to the community college, this is where they get their training. This where they get their upskilling. So, it's not like we're just talking about newbies out of high school who need to get Tech 101. We're talking about a lot of high-level professional stuff. But it's a mixture, and it's all over the place.

So, with that confusion being the background, I'd like to turn it over to Markus to go ahead and make sense out of it.

[00:30:54]

IT Cybersecurity Model Curriculum for California Community Colleges

Markus Geissler, PhD

- Professor, Computer Information Science, Cosumnes River College
- Chair, C-ID IT/IS Faculty Discipline Review Group
- Vice-chair, ACM Committee for Computing Education in Community Colleges (CCECC)

Richard Grotegut

- Regional Director/Employment Engagement, ICT/Digital Media Sector, Bay Region
- Lecturer, San José State University
- Computer Science Professor Emeritus, Ohlone College
- Director, Western Academy Support & Training Center (WASTC)

MARKUS GEISSLER: Well, thank you very much, Steve. I appreciate being included and allow me to introduce myself briefly, but also you may not know. I am the Chair of the IT/IS FDRG for the CID process. Let me take that apart. That is the Information Technology and Information Systems Faculty Discipline Review Group that has been established, was established about seven years ago, when the CID process first started.

And for those of you who may not know what CID is, it is the course identification superstructure that was developed by the academic senates of both the California Community Colleges and the California State Universities, with an invitation to the UCs, who have been at the table less than more but who have been there as well, to get together and find ways to share curriculum across the two- and four-year programs. And very fortunately, and thank goodness that has also, to a good extent, been adopted by the K12 system as they feed into some of our systems, and I'll elaborate on that in just a second.

I want to give Richard, who has been working on this FDRG with me since the very beginning, I'll produce the opportunity to introduce himself here. Richard…

RICHARD GROTEGUT: Yeah, thank you, Markus and Steve. Thanks, everybody. Yeah, this has really been an endeavor of mine when I began teaching, was these pathways in IT. It's been almost a

thirty-year-long kind of goal to have this happen. So, I jumped at the opportunity to serve on the FDRG with Markus and everyone. We've made a lot of headway; we're just looking for the CSUs that want to partner with us and make it happen. So, thank you.

MARKUS GEISSLER: All right, thank you, Richard.

[00:33:06]

IT-Related C-ID Model Curricula

- Created as part of C-ID process
- IT Cybersecurity Model Curriculum DRAFT (developed in 2018; 21+ units)
    - 3 Cybersecurity Core courses
    - 3 Cybersecurity electives
    - 1 Programming or Scripting elective
    - Compatible with programs seeking DHS/NSA CAE-CD designation
- Based on IT Model Curriculum (finalized in 2015; 22+ units)
    - 4 IT Core courses
    - 2 IT electives
    - 1 MATH elective

MARKUS GEISSLER: Really quickly, before I get started, more kudos to Keith Clement. We would not be here as the state of California with many CSUs now launching cybersecurity programs. Not that some haven't already had them, but the pushing forward, the driving of this effort is squarely on Keith's shoulders, so many kudos and credit where credit is due. We wouldn't be talking about what we have and where we want to go if it hadn't been for him. There's certainly… We're not at the end, and I'm not sure if we ever will be as our field keeps moving, but he deserves a ton of credit for this, so kudos from this end as well.

I'll talk about the C-ID side as it pertains to the community colleges and those with whom we interact, which, again, is our K12 partners as well as our four-year partners.

But one of the toughest parts that we've encountered as members of the FDRG was that, when we came up both with the IT Model Curriculum in 2015, and that's been finalized and been implemented, and then later on with the Cybersecurity Model Curriculum, which for similar reasons has not yet been approved, and it's institutional—it was mentioned earlier that things just

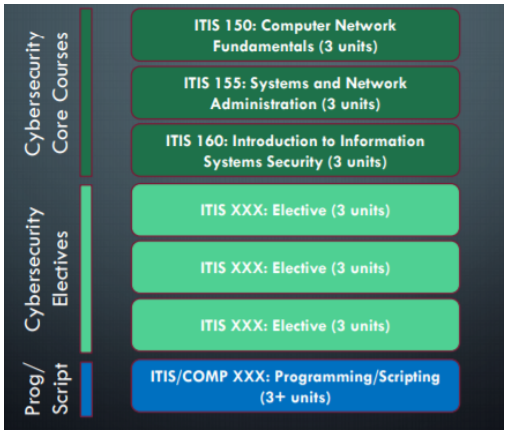
move relatively quickly in the industry and relatively slowly in academia. We're academia, and we're oftentimes not able to keep pace, so that's why we're looking at a draft curriculum for cybersecurity, but we need to make sure that this is all used across the different sectors.

And let me first talk about the IT Model Curriculum at the bottom… Four core courses (the Core Four, as I call them), two electives, and then a math component, and then going back up. I'll talk about the IT Cybersecurity Model Curriculum in substantially more detail, where we've got three cybersecurity core courses that I'll introduce in just a second, three electives, and then another elective in programming or scripting.

One thing I'll be pointing out as we go is that the curriculum that was designed is compatible with the CAE-CD designation that many colleges are seeking that only very few colleges in California have earned to date. I'll talk about that as we go as well, and the different components that make up that additional goal for many of our community colleges.

[00:35:36]

C-ID Information Technology Cybersecurity Model Curriculum (DRAFT)



MARKUS GEISSLER: So, three core courses, and the IT/IS (again, Information Technology/Information Systems) designation within the C-ID process. The first one here is

Computer Network Fundamentals. I'll talk about that in just a second, but fundamentally compatible with the Network+ certification by CompTIA and very similar to Cisco's CCNA 1 course.

ITIS 155 helps to prepare students for the Server+ CompTIA certification. Or if you're going to go with a vendor-specific site for some of the initial Microsoft certifications or Linux certifications. And then ITIS 160 helps prepare students for the CompTIA Security+ certification.

More general, but those are the core three courses that the FDRG, along with input from many other academics and industry partners, deemed that those will be skills that every IT Cybersecurity professional should have, certainly at the two-year level.

Beyond that, we've got three electives, and there are actually eleven possible electives like this that colleges can offer. But in order to offer a two-year degree, associate degree, or a certificate for folks that may already have other degrees, there will be three required electives to be taken of that selection of eleven.

And then we have a programming and scripting course for a total of what I'm going to call 21+ units because, as many of us know, some of the programming courses, especially those in Computer Science, where we've had a very difficult time implementing the ADT because of the high unit values of some of the science and some of the programming courses, but that's where the + comes in. But this is actually a minimum of 21 units. It can be done that way, but at some institutions, it's just going to be more than that.

[00:37:40]

ITIS 150: Computer Network Fundamentals (3 Units)

- Prepare students for CompTIA® Network+ exams
- Consider integration with Cisco Networking Academy courses (CCNA1v7)
- DHS/NSA CAE-CD Course #2

MARKUS GEISSLER: So, ITIS 150 is the course number #2 (I'll get to #1 later on. I didn't forget #1) for CAE preparation, but it also is basically that foundation, right? I heard a gentleman at Cisco at

one of the winter conferences say a few years ago, “Without the network, there’s no cyber,” so people need to understand how networks work.

Now, can that course be taught at K12? Absolutely. It is being, it has been, oftentimes with the Cisco curriculum. Have I seen it taught in the upper division at a CSU? Yes, I have as well, very interestingly. So, one of the major components that we need to talk about throughout this is the coordination between what’s taught, where, to which level, but that’s 150.

[00:38:35]

ITIS 155: Systems and Network Administration

- Build, maintain, troubleshoot and support server hardware and software technologies
- Prepare students for CompTIA® Server+ exam
- Consider integration with Microsoft IT Academy courses
- DHS/NSA CAE-CD Course #3

MARKUS GEISSLER: Again, server, hardware, software, technologies… Course #3 for CAE-CD, and that is, again, Microsoft or Server+ or Linux.

[00:38:51]

ITIS 160: Introduction to Information Systems

- Fundamental principles and topics of Information Technology Security and Risk Management
- Helps to prepare students for CompTIA® Security+ exam
- Advisory: Computer Network Fundamentals (ITIS 150)
- DHS/NSA CAE-CD Course #4

MARKUS GEISSLER: And then the third core course is the Security+ exam preparation. Notice there’s advisory here. We’ve been very careful not to implement prerequisites, oftentimes because of industry folks coming back in. But certainly, if somebody were to take this course without having at least some background in networking, that would probably be at a disadvantage to be able to successfully complete this third course of the core three for the IT Cybersecurity Model Curriculum.

[00:39:25]

C-ID IT Cybersecurity Model Curriculum (DRAFT) Cybersecurity Electives

- ITIS 148: IT Risk Management (3 units) – DRAFT
- ITIS 151: Routing and Switching Essentials (3 units)
- ITIS 152: Network Security and Automation (3 units) – DRAFT
- ITIS 161: Cybersecurity Analysis (3 units) – DRAFT
- ITIS 164: Introduction to Cybersecurity - Ethical Hacking (3 units)
- ITIS 165: Computer Forensics Fundamentals (3 units)

MARKUS GEISSLER: Now, before I move on too much more quickly, you'll see the word 'draft' on quite a few of these descriptors, as well as on the Cybersecurity Model Curriculum. And the reason, again, that it's a draft is because it is… I'm not going to say stuck in committee, but there has been a relatively slow process that we're dealing with as part of the C-ID effort. I'm very happy to say they are forming an advisory committee. I was asked to become a member of that, and that will be one of my main tasks, is to make sure that the five-year cycle that may work well for English and for Physics and for History is probably not going to be the ideal type of review for a field that moves as quickly as ours, certainly in Cybersecurity these days.

Here you'll see the first six electives for the IT Cybersecurity Model Curriculum. The reason that some of them are not drafts is that they're part of the IT Model Curriculum as well, so there's definitely a way to move from one to the other, and it's designed that way. And we've got everything from additional Cisco courses when it comes to the routing switching and network security and automation, and then you've got forensics there.

- ITIS 166: Cybersecurity Operations - CCNA CyberOps (3 units) – DRAFT
- ITIS 167: Network Security - CCNA Security (3 units) – DRAFT
- ITIS 168: IoT Security (3 units) – DRAFT
- ITIS 170: Cloud Computing and Virtualization (3 units) – DRAFT
- ITIS 171: Cloud Security Fundamentals (3 units) – DRAFT

And page 2 of 2 of the potential electives that can be offered, again, all the way K through 12, all the way through the baccalaureate program or, frankly, even beyond. I'm not saying I've seen some of the courses at the Master's level, but I wouldn't be surprised, depending on some of these more advanced cybersecurity ops kind of courses, for example. And yes, the cloud very

much is in here as well, not only from an implementation but also from a cybersecurity perspective.

[00:41:11]

C-ID IT Cybersecurity Model Curriculum (DRAFT) Programming/Scripting Electives

- ITIS 130: Introduction to Programming Concepts and Methodologies (3 units)
- COMP 112: Introduction to Programming Concepts and Methodologies (3 units)
- COMP 122: Programming Concepts & Methodology I (CS1) (3 units)
- ITIS 135: Linux Shell Scripting and Programming (3 units)
- ITIS 136: Python Programming for Cyber Security (3 units)

MARKUS GEISSLER: Finally, here's your #1 for CAE-CD. So, we've covered all four courses that they told us for the IT Model Curriculum would prepare colleges for the core requirements. And this is some kind of programming course as both the industry told us as well as is necessary for many of the operations for folks to be successful.

So, we'll take not only the ITIS 130 descriptor. We'll also take Computer Science descriptors. We do know that students who are regularly advised into Computer Science because that's oftentimes the horizon of many counselors when it comes to computing. They don't think about some of the other disciplines, but they know Computer Science. But then some students may not find the need or, frankly, the ability here on there as well in Calculus and in higher level math.

And if you notice, by the way, contrary to the IT Model Curriculum, which had basically any course above Algebra II as a requirement, there's no math in this as a requirement. We recommend Statistics because that's helpful in analyzing reports, but it's not required.

Now, again, why do we have this many electives, this many options? Because industry needs maybe different local faculty expertise. Existing other programs may be different, so we definitely want this to be as seamless as possible.

Now, before I finish a couple of questions, I'd also like to address something that came up in a meeting yesterday. And Keith mentioned earlier—how about this hands-on, right? Is this all

just theory? And for those of you who may be teaching some of these course, the great majority of them are implemented with substantial lab components, so the hands-on is definitely there, and that's where students pick up, hopefully, some of those professional skills as well. A lot of companies hire for attitude in addition to some skill. Frankly, a lot of them hire for attitude and then teach the skill, so we have opportunities within our interactions not only in the classroom, virtual or physical, but also during that lab time, to make sure that students can interact.

And then that question that keeps coming up—is a two-year degree enough? And the short answer is, for many jobs for students to get started, yes, it probably is. But many of us have experienced… I've been a long-time professor at Cosumnes River College as well. Students who have come back and said, "Hey, I got my Networking degree, I've got my IT degree, where can I get my bachelor's?" and we haven't had very good answers to that question. Some of our private colleagues, of course, like National that was mentioned a while ago, have been there, but boy, would we love to send them to our CSU partners, and it looks like, as soon as they implement some of those programs, we should be able to do so as quickly as possible.

One other thing that I would encourage… There weren't too many CSU folks on this call, but I'll mention it anyway for the record. You know, even though we deal with 60-unit degrees, the CSUs can't accept more than 60 units. So, one of the big coordination pieces that I believe needs to be handled locally, between the community colleges that can implement in various flavors of this model curriculum and our CSU partners, is, well, some of these electives that may go beyond the basic lower division requirements that a CSU might implement for a cybersecurity program—can those skills actually, with maybe a certain degree of validation, count for upper division credit? Or at least beyond the 60… You know, up to 70 units?

And that's where that local collaboration will continue to need to be very, very important so that we can make sure that, for every region within our state, for the local needs and, again, for the expertise that makes this at the CSU level as well. We've got solutions for our students that will allow them to easily move from one educational structure to another. And the same, by the way, goes for K12 to community colleges as well.

These descriptors do align to industry certifications. Many of them do. And if we keep using that to a great extent as a guide as to need to update them, but also as a target to which we can work, then I think we're best serving our students.

Richard, would you like to add anything before we open it up for questions?

RICHARD GROTEGUT: No, not much, really, Markus. Great job kind of summarizing our work. You know, like I said at the beginning, this has been a long-time goal for me, and I was teacher at Ohlone College for twenty years, trying to find a place for our students to go to as well.

We are a community college, and that's what I really like about the model, is that it has something for everyone. It has a place for our students who have degrees, many of them, and come back to get training to upskill, and it has opportunities for them to do that.

It's also been a great tool to advise our high school partners and to inform our competitions that we do, summer camps that we do every summer, as outreach. The content comes from the curriculum that's based in this model. So, I'm thrilled to be a part. I love having the CSUs. I'd have to say I did join the ranks of the CSU instructors, and that's kind of helped the articulation process a little bit, too, at San Jose State, so…

STEVE WRIGHT: Thank you much for these comments and sharing the curriculum. I think it begs a lot of questions—like, if this the lower division, what does the upper division look like? And I know that Nancy Johnson actually addressed that and put together a model for the upper division. Increasingly, we look at project management skills and all these other things because, if you have this as a base, then the next is…

[00:47:20]

Wrap-Up and Questions

STEVE WRIGHT: But we don't know yet. I mean, that's a lot of wonderful things, and right now, I'd like to ask Nicole to go ahead and kick off our final survey after you've heard everything. We're interested in this group's feelings about this kind of interconnection. And we'll take a look at those results and have any final questions.

So, does this cybersecurity framework and curriculum standardization efforts seem like a good model to integrate the public and private educational efforts for California?

Speaking to Keith's thing, I mean, we're expecting everybody to say yes…

And the next one has to do with *do you believe the California Community College system IT Cybersecurity Model Curriculum should be transferrable to the CSUs?*

Yeah, I mean, this is kind of important. If it was transferrable, how much do you think people would take advantage of it? I, personally… You know, I've been betting for a long time—if we could open up that pipeline, we could get a ton of people. But you know, people might say no.

And the credit for prior learning—we definitely need your input on that because we have just so many people that get certificates off of self-learning or maybe something in the military or whatever, and there comes a time when technology advances this rapidly that the academic institutions just kind of have to open up their mind a little bit to the fact that there might be another more porous way to go about doing this. So, getting your vote on that is very helpful, so I think we're pretty much voted… OK.

KEITH CLEMENT: I love those remarks, I've got to tell you. I have spoken to so many folks in industry—not putting anybody down. I've spoken to so many folks in industry that seem to think that we could, on the education side, just make change happen overnight, right? I mean, I hear that so often. Like, "We tell you what we want continually, yet you still haven't done what we've

been asking for forever." And it's like, "Actually, we appreciate what you've been telling us, but we need to do this in a more coordinated, systematic, and organization fashion on a regular basis. So, you might have sat down with us in 1989 and told us what your firm was really looking for then, but a lot has changed."

And Steve, to that point, I don't even know if a yearly annual review meeting is going to be fast enough to keep up with the way that industry moves so quickly. I was on a call the other day where basically said, "I was told the term 'database' is over, and it's now called 'the cloud,' and that they're objecting to the use of the term because it's no longer accurate, in their perspective at least. That's how fast things change. Who would have thought that 'database' or 'dbase' or any of those terms is already in the IT museum of ancient terms, right? Wow.

STEVE WRIGHT: Yeah, I think that's… Well, and I was reading an article this morning about a job that a company had last year, they called it a Data Analyst or Data Scientist. This year, it's called a Cybersecurity Analyst—and it's the same job! So, it just depends on how the person is used. So, the skills may actually, you know, one thing, and then how you're being used in the company and where the emphasis is, is another. And technology—you know we love to change names very quickly. I mean, I remember back in my days with Verizon and everything, everybody was talking about convergence, you know? Like they're going to put everything together. I don't hear 'convergence' anymore, you know? Just all these different types of technology change, and the jobs change, so we do have a moving target.

So, keeping in touch, as you said, Keith, with industry and finding out what they're calling it, but then breaking it down and just aggregating it to the essential skills—that's why I keep coming back to it… No matter how much more everything advances, I go back to the work that Markus and Richard and Olivia have already done on these curriculum skillsets—nothing has really changed. You still need to know that stuff.

KEITH CLEMENT: Olivia and I were on a recent phone call the other day, where we're actually looking at the development of a menu-based curriculum skillset. We have kittens—I apologize if they're distracting. They're tearing up my office right now.

A curriculum skillset that is actually done on a menu-based motif, where industry or occupational sectors or position types could actually pick and choose the specific skill competencies that work for them and their company, at their firm, at their government agency, or whatever. And that would be very wide and open.

And I do mean an a la carte menu—we would have some basic fundamentals that would service competencies across all sectors. We need to have people that can write oral communication, right? I mean, that's a skill for many people. But then we would have this other skillset that would be menu based, and they would pick and choose from which ones served them and their agencies and companies, and which ones did not.

OLIVIA: Yeah, there was a question in the chat box saying, well, you know, "Certain apprenticeships might not work in private versus civil service," and that's exactly the reason why we're developing MITCs that have the major job functions for each standard occupational code, like for cybersecurity. But then the particular employer taking advantage of that apprenticeship could take a look at the job functions and the competencies associated with that job function and match it to what they want their journeyperson to be once they've completed the program. So, that's why I think the MITC approach to defining apprenticeships really makes it flexible for employers.

AUDIENCE MEMBER: What's MITC, Olivia?

OLIVIA: Minimum industry training criteria—it's a division of apprenticeship standards term.

MARKUS GEISSLER: Also, one more thing, looking at the chat, too—and I'll go on record with this. A lot of us are concerned about the curriculum updates and how long it takes with our colleges, and it's a problem, no doubt about it. But you know what? If I ever get castigated, even though my own curriculum stills says I should be teaching this, and I have actually taken the initiative to update the curriculum, and I'm teaching the newer version, then I would probably realize that I'm in the wrong place because it can't be more important to follow what's in the syllabus than to make sure our students get current content.

So, yes, we need to do good work, the curriculum work, and trust me—we in the FDRG try to keep those descriptors as currentnas possible, but that said, make sure that your students get the current knowledge that they need to be able to function not only as transfers but in the job market.

STEVE WRIGHT: Well, thank you, Markus. And Keith, if we can give you the last word, could you tell us what we can do to help you, going forward?

KEITH CLEMENT: You know, having conversations and meetings like this is exactly the way that we move forward. It is key that we have all sized businesses (small, medium, and large businesses) working in tandem with our K12, two-year, four-year partners, in conjunction with our government agencies and organizations. And when we are all synchronized and on the same page, we will have this problem solved. And otherwise, you know, we'll have this discussion in ten years or whatever, right?

So, thank you very much for having me. I deeply appreciate all that you do, Steve and Markus, Richard, Olivia, and all of you. It's great to see everybody today.

STEVE WRIGHT: Well, thank you very much, Keith and Markus and Richard, for your presentations today. We'll wrap it up right now. Within a week, we should have this finalized, edited, transcribed, original PowerPoints, all the various links that everybody mentioned today, as well as Keith's papers, on our website for your archival utilization. Thank you very much. So long!