**Building a Cyber-Savvy Workforce**

***Presented by:***

**Pam Frugoli, U.S. Department of Labor - ETA
 &**

**Mitch Sepaugh, Cleveland Community College**

**Pam Frugoli**: Welcome to “Building a Cyber-Savvy Workforce.”

Thank you for joining us today for this webinar. I am Pam Frugoli. I’m team lead for the O\*NET system and the industry competency models project here at the US Department of Labor, Employment and Training Administration. Joining me today is Mitchell Sepaugh, who is the Project Manager of Industrial Systems at the National Consortium for Mission Critical Operations. It is housed at Cleveland Community College (CCC) in Shelby, North Carolina. Mitch has extensive experience as an OEM automation systems integrator, and is currently responsible for development of the Mission Critical Operations curriculum for Cleveland Community College as part of a U.S. Department of Labor grant funded initiative. Previously, he was responsible for developing the first Automation Engineering Technology curriculum based on the Automation Federation’s Automation competency model.

Our webinar today will cover the following topics. We will start with an in-depth discussion from Mitch about what are mission critical operations, and what are the competencies required of workers to keep those systems operating. Following that, I will provide some context about the broader industry competency model initiative at the Department of Labor and about the resources that are available to users, through the DOL-sponsored website, which we call the Competency Model Clearinghouse.

So here’s what you can expect to get out of this webinar today. One is the importance of cybersecurity and the role of the cyber-savvy workforce; and using the models – the competency models – to support mission critical operations; and finally, using the Competency Model Clearinghouse.

Now I’d like to turn it over to Mitch Sepaugh, our subject matter expert. Take it away, Mitch.

**Mitch Sepaugh**: Thank you, Pam. Mission Critical Operations is a part of a U.S. Department of Labor TAACCCT grant. The TAACCCT grant was awarded October 1st, 2013. Cleveland Community College is the lead community college in a consortium of colleges. The consortium together was awarded 23.2 million dollars. The primary purpose of the grant was to develop a training program for mission critical operations. The grant started in 2013 so right now we are wrapping up our second year, and year 4 of the grant is for data collection and reporting of outcomes – three active years in the grant.

One of the things that we get asked most frequently is, when we start discussing mission critical operations, is what exactly our mission critical operations. And working with our partners in the consortium and also with our industry representative partners, we basically define mission critical operations as: *“Any operation that requires round-the-clock supervision of systems and is aimed at combating the evolving threat of critical infrastructure operations failure.”*

These failures can come in a number of different ways. They can come through a cyber-security breach that effectively shuts down or handicaps a piece of equipment. They can come as a result of a natural disaster such as a flood or a hurricane or a tornado. They can come as a result of a power outage in a black-out or brown-out scenario. So there’s a number of different things that could come about that could bring down a technology-dependent business. These operations may involve different technologies in different industries: Power industry, transportation, and manufacturing.

These are all systems and these are all industries that run 24 hours a day, 7 days a week. They’re all different sectors, they are all mission critical though.

The Department of Homeland Security identified 16 different industry sectors that are vital to the national economy and our way of life every day and those sectors all share some type of technology between the different sectors. And that common approach to the technology and the common technology that is used in the different sectors is really where the focus of mission critical operations runs. Whether that is supplying power to a hospital, supplying power to a manufacturing facility, whether it is keeping a data center up and running so that everyone can log in to their favorite web site, keeping the stock exchange running, whatever it might be, one thing that we’re learning is that all of these sectors are interdependent and relying upon each other.

Five key mission critical competency areas were identified and defined for the grant by our subject matter experts working with us as we develop these competencies. These five primary competencies are shown here. The operations management competency is the ability to look at a system or a sequence of systems in either a single facility or in a group of facilities and be able to see what the situation calls for as far as the use of technology, the modification of the technologies that are in place, the communication between the different systems, and being able to optimize the operations of those systems of technology.

Operations management, of course, comes from the ability to apply Situational Awareness. Situational Awareness comes into play based on, not just what a particular piece of equipment is for, but when that particular piece of equipment is called for, how is it used? For example, a back-up generator. Backup generators are typically not very important until you need it. Once it kicks in then it becomes certainly a mission critical piece of technology.

Understanding how the situational awareness plays into daily operations in a given industry or given facility directly plays a role in the Incident Response as well. Incident Response is basically knowing how to handle an emergency at a particular time, based on what the nature of that emergency is. So understanding what the situation, understanding what the problem is, and then being able to go into an automatic mode where you know what to do, you know when to do it, you know who to call, and what the ramifications are going to be after an incident takes place in order to get the systems back on line with as minimal a disruption as possible. Of course, being able to be very skilled in the incident response goes a long way with understanding and knowing what the capabilities are and what the operational status is of your technology and that comes as a direct result of preventive and predictive maintenance.

Being able to apply preventive and predictive maintenance schedules, a competent professional has a feel for how that technology works when it’s working properly, how it interfaces and integrates with other pieces of technology; and what the different interdependencies are of these various systems. How does the power system affect the air conditioning system, how does air conditioning affect transportation and communication systems by being able to keep network servers online. So understanding the interdependence of these different systems, being able to anticipate incidents or potential failures because you’ve been watching these systems and how these systems operate on a regular basis, and be able to identify what the best practices are to keep those systems operating at their optimized and most efficient manner.

And of course the last bullet here is cybersecurity. So many of these different systems now have to communicate amongst themselves in converged networks, a lot of the physical layers of these networks are Ethernet or fiber optics with radio communications between different sites, and so these technologies in the past have been lots of different kinds of technologies, but now they all have a common interface, and that is the Internet. So each of these different systems can really wreak havoc not only within their own system, but also they can start having impact on other systems as well, if these systems are tampered with. So being able to keep these systems protected is a key element in the cybersecurity world. We don’t want to take down a piece of IT equipment and have that then affect a piece of operational equipment, but then we also don’t want to take down a piece of operational equipment if that affects something in the IT realm. And understanding how these pieces play off of each other is key to the mission critical competencies.

When we started working with the competency models, we started off working with a familiar model that we had already worked with before in the mission critical field and that was the Federation’s Automation competency model. And this was a model that we had used previously, as Pam mentioned, on our development of the Automation engineering technology program here at the college.

There’s a block on Tier 4 of the Automation Competency Model that refers to Operations Management. In that block, there are certain critical work functions that are identified. These critical work functions have to do with developing the industrial process, and the production plans and their documentation, what protocols are in place, so if you have new staff that come on board that can pick right up into the game plan and move things along without having to have a lapse in systems operations. This allows support for the operation in control of whatever the production or the process is and what the equipment is. In order to be able to maintain that equipment and keep it working in an optimal form, monitoring plays a big role in this, so being able to monitor these processes and these systems, identify these recurring patterns, and then being able to use those information and those recurring patterns to be able to manage the continuous improvement process. Always looking for a better way to do something and optimize something can directly affect the company’s bottom line. Managing raw materials, the consumables and, of course, the outputs and the production of whatever the business is or the entity is, you can get more production and more performance out of the system when everything and everyone that’s in the system is operating at a peak performance level. So many different things are automated processes today, that this industrial process and applications and operations can apply to things we have always traditionally thought of as industries such as manufacturing, but a lot of these processes also occur to things that are not traditionally thought of as an industry such as utilities, transportation, and so forth.

The situational awareness competency that is part of the Mission Critical Operations was adopted from some of the other competency models and it’s named explicitly on the Engineering Competency Model, developed in collaboration with the American Association of Engineering Societies and its member societies.

Situational awareness involves identifying different alternatives—and how can we solve this particular problem, or how can we approach this particular task at hand, and how can we get the system back online in the fastest, most reliable manner. So choosing from the different solutions that are presented during this brainstorming situational awareness activity, and choosing which one of those is going to be the best one is the core function of Mission Critical Operations. So the problem solving; the prevention of problems; the decision making; being able to identify the problem; locate, gather, and organizing the relevant information; generating alternatives; choosing a solution; and then implementing the solution – all of that in the most efficient and fastest manner possible.

Tying in with the incident response bullet from earlier, we looked to the Cybersecurity Model. The Cybersecurity Model was put together by NICE. In a cybersecurity incident, we need to be able to look at whatever the incident is to be able to remediate that incident as fast as possible. If you have a key server go down, large areas of the country could go dark as far as the Internet is concerned. But it’s not just about being able to maintain Internet access. Mission critical operations would need to be maintained in the face of such an outage. Servers are not always running web sites – sometimes they’re running communications outfits. So whether it’s radio communications for emergency responders; whether it’s telecommunications companies and keeping our cell phones actives; these pieces of equipment are something we depend on for daily operation and even for disaster recovery. So those technologies need to operate all the time.

So the incidence response is part of about developing and knowing what is the business continuity plan to recover as quickly as possible and here we have answers to such questions such as “How are we going to communicate? Is the public going to be affected? How much is the public going to be effected or is this just something that’s local?”

Being able to look at and review what happened after the incident is over and after the event has been cleared, then you can run through a post-incident analysis. And in that case you want to determine what caused the issue; how can we prevent that issue from happening again in the future?

So the KSAs – the knowledge, skills, and abilities – needed to respond and remediate an incident, and restore functionality to the system, such as the Business Continuity Plan Implementation, Crisis Communication, and the Post Incident Activities and Analysis, are all critical features in the Incident Response block.

For Preventive and Predictive Maintenance, we go back and revisit the Automation Federation’s Automation Competency Model. There is a block here for the predictive and preventive maintenance. Critical Work Functions in this block, located on Tier four of the model, include the supporting and the installation, the customization and upgrading of equipment, different equipment as new technologies emerge, our needs for customizing pieces of equipment in a given installation or for upgrading equipment so that we have more tools at our disposal. So particular tasks that have a specific purpose, and over time these can be customized, not only need to be able to upgrade the equipment, but you also need to be able to update the documentation so that that you can reflect those changes. A person that puts the changes in today may not necessarily be the person that has to go back and do some maintenance or do some repair work at a later time. So documentation and being able to transfer that knowledge is very key.

Being able to utilize predictive maintenance techniques gives a mission critical operator the ability to learn that after so many hours of run time, certain maintenance things need to be performed—whether it’s lubricating bearings, whether it’s changing cables out, whether it’s flushing server memory, whatever the case may be; being able to look at and monitor those systems for where the best practices can come into play can have a huge impact on the optimization of a system.

So this helps the process or the production run as smoothly as possible. And when something does come up that something doesn't run very smooth, it allows you to be able identify, diagnose, and repair those problems when those anomalies arrive – being able to communicate with others to ensure that maintenance and repairs meet the operational needs without making the problem any worse and with a minimum disruption in services. Sometimes that can include scheduled down time so that you can perform these maintenance activities in a controlled environment.

In order to do this, there is a lot of hands-on knowledge and requirement of these equipment operations that if someone is not involved on a regular basis with the equipment, they need to have some familiarity through it through regular maintenance. If they don’t have regular interface with the equipment, then it’s a new deal every time they walk in and that can delay successful remediation of an issue.

Being able to use preventive and predictive maintenance also means that the – not just the equipment that’s out there but also the tools, the systems, and the workstations —you know, making sure if you use a laptop to connect to a piece of equipment, that your software licenses haven’t expired. There’s a really bad feeling when you go to connect to a piece of equipment and your software doesn’t work. So being able to understand how this daily interaction with your equipment has an impact on critical operations is key.

Recent update to the Automation Model – in the Automation Competency Model – added a cybersecurity block. This cybersecurity block is a concentration in the automation program, but it also shows up in the IT model and of course there's the entire Cybersecurity Model that can expand on that even further. The difference between cybersecurity in the realms of Information Technology and Operations Technology has a lot to do with the environment and the application, where the cybersecurity is being used at. Whether it’s Information Technology, IT, or whether it’s Operations Technology, or OT, there's network connections in use – they both have switches they both have routers; there’s both server equipment in place, but the requirements and specifications for a plant floor is much different from that in an office environment.

They operate the same way but they don’t operate for the same reasons. And they were not installed with the same specifications and requirements. So being able to understand how that piece of equipment will impact the systems around it is a huge part of being involved in mission critical operations. If you simply shut down a computer in an office suite, you may put one particular person out of work for a little bit while that computer’s shut down. If you shut down a computer on a manufacturing floor, you may shut down the entire production floor and it could take hours to get that system back online, so understanding the impact of what it is that you’re doing, and what the ripple effects of it are very huge. And that goes back to the situational awareness we spoke of earlier.

So Critical Work Functions here include differentiating between IT and OT architecture, and the operation of these architectures; determining and implementing the appropriate tools and methods for industrial automation control systems; cybersecurity; understanding zones and conduits of information; understanding how the system is laid out, and what its architecture looks like; being able to understand security levels in each zone and which of the parts of the system are more critical than other systems are plays a role in risk management and being able to minimize risk should a particular piece of the network go down; being able to look at security and information assurance fundamentals; who has access to the equipment – if they have access to something, how much access do they have? Is it read-only? Is it something that they can make changes to? What is the business resiliency of the particular system or of the particular network? What is the continuity plan in place should there be a mishap? And then of course, and sometimes, depending on that the application is and depending on what the breach is, the incident could actually have legal ramifications, which could involve federal government regulations or could trigger investigations with compliance auditors or whatever. So being able to understand what those changes are and again what the implications are if such action is is a huge factor.

References back to the Cybersecurity Model and, again, depending on what the application is, a given individual may need to go into a deeper dive into a particular instance – whether it’s in the office space area that controls the manufacturing facility, whether it’s in the production floor of a facility or whatever, the different aspects and implementations of the network play a role in the cybersecurity aspect of it. And cybersecurity is not always making sure that your passwords are changed. Cybersecurity can also include elements of physical security – making sure the door to the server room is locked; making sure no one has access to a particular building; making sure you have offsite storage for your backups in case of a fire or natural disaster. All of those play a role in cybersecurity, so it’s not just making sure you have your password changed every 60 days.

Project outcomes for this grant is to develop an Associate in Applied Science degree in mission critical operations. Working with our partners in the grant, the other schools, we’ve come together with different sets of academic competencies that are required to make sure that we’re all in compliance with each other and that we can all work toward a common academic goal. But then also working out what the job-related competencies are that are coming from our industry representatives.

The 3 other community colleges that are working with us in this grant are Wake Technical Community College in Raleigh, North Carolina; Nash Community College in Rocky Mount, North Carolina; and Southern Regional Technical College in Tifton, Georgia. These community colleges are all working towards the associate degree level. We’re also working on the diploma and certificate levels as well. And of course we have our university partner is University of North Carolina at Charlotte, located in Charlotte, North Carolina. Charlotte is a partner with us on the grant, partly because they’re a Cybersecurity Center of Excellence, but also because they offer us the advice and knowledge for creating a pathway from the 2-year associates degree up to the baccalaureate studies, to the bachelor of science degree. And of course once the transition has been made from associate’s degree to bachelor’s degree at the university level, then there’s options to go on and pursue graduate studies as well.

As students move out into the mission critical operations world and take up positions in the workforce, we need to be able to track them – part of the requirements of the grant. So for those already working in the field we want to find out: did they get promotions? Did they get raises with those promotions? Did they just get raises? If they weren’t working in the field, were they able to get a job in the field and what was the difference in the workforce and in the manpower that’s being made available in these mission critical areas, in all the different sectors that are out there.

So one of the ways we’re trying to track our students and benefit our students is not just on the academic curriculum side but also on the professional certification and professional credential side. We’re developing two different professional credentials with industry resources. We’re working in collaboration with CompTIA . You may have seen CompTIA’s name mentioned on the IT Competency Model earlier. CompTIA’s working with us on the development of the Certified Mission Critical Operator or CMCO certification. This is mostly an identify and recall type of certification, where someone can go in and they can identify a piece of equipment and what that piece of equipment’s primary application is. So they can identify this is a piece of air conditioning equipment; this is a piece of computer equipment; this is networking equipment; it’s communication equipment; it’s power equipment and so forth. They can identify what the piece of equipment is and what its primary function is and overall have an idea of where it plays a role in the mission critical technology family.

We are also developing a second-level certification: the Certified Mission Critical Professional, or CMCP, which is being developed along with the International Society of Automation (ISA). The second-level certification is being developed to not only have an individual be able to identify and recall what a particular piece of equipment and what it does, but why that particular piece of equipment may be considered mission critical versus important, or simply something that’s nice to have. Being able to put that piece of equipment in context, in a particular scenario or in a particular situation and be able to determine what needs to happen in response to either maintaining that equipment or getting that equipment back online, or in some cases even procuring that equipment so it can meet a need that’s not currently being met. Those are the tasks that we’re looking at in a certified mission critical professional.

One of the things that are subject matter experts had concerns with, which helped prompt the development of this program, is the ability to capture and pass on the institutional knowledge and the lessons learned by those individuals that are currently working in the field but may be retiring out or may be transferring into other sectors that aren’t directly related to the technology. So to be able to support and capture that knowledge base that’s out there, we needed to try to put the students into as much of an immersive environment as we can possible put them for the folks that are going to work in that field. And one thing that our subject matter experts refer to was the ability that being able to sit in one location in an operations control center or in a command room and be able to work at other pieces of equipment throughout a facility or even at another facility within the company was something that was just done every day now. And so whether it goes by different names, whether it’s remote operation, or whether it’s telepresence, the ability to be in one location and work on equipment that’s in another location is an expected skill trait now. So we wanted to be able to put that telepresence capability in our classrooms as well to help support the development of this program. Especially with this being a very new program, being a very unique program in the country, we were going to have students that were going to be not local to our campuses, and so being able to have the telepresence, not only for our local students to understand how to work in that remote operation or that telepresence environment, but also to be able to reach out to students that are not on campus and have them be able to remote in to equipment that’s on our campuses just further closes the loop between what the training needs to be, not only for the students but also for when they get out in industry. This way they don’t see this technology or this capability for the first time when they get out in the field – they’ve already been exposed to it, and they’re already comfortable working in that familiar surroundings.

As a final part of the grant, we needed to be able to develop curriculum resources to support the classroom instruction that we’re having and also the professional development that we’re having. There are not a lot of textbook resources or there’s not a lot of educational resources out there that specifically address mission critical operations – there are things out there for the individual technologies but they don’t necessarily put those technologies in the context that they need to be put in that make that piece of technology a mission critical piece of technology. So as we’re developing resources to go along with this project, these resources are going to be released as open educational resources or OER and these will then be posted on the Skills Commons.org web site. The resources in open are being released under Creative Commons licensing through the CCBY standards. There are essentially like an open source, public domain resources – after all, being funded by DOL, they are public funds, so if someone wants to be able to use these resources either for themselves individually or use them for their institution or use them for customers that they may have or providing training or professional development for that mission critical operator, these resources will be available to help get things started. They can either adopt these pieces of resources – they can either adopt them wholly as they are; they can embed them or integrate them with existing training resources; or they can adapt them and update them as the technology changes and evolves for whatever the current applications are.

The National Consortium for Mission Critical Operation or NCMCO is the name of the organization that we have created here. Our schools that are the initial partners in this, of course Cleveland Community College is the lead school, is who I’m with. Wake Tech, Nash, Southern Regional, and UNC Charlotte are our partners.

[Cleveland Community College, Shelby, NC – Lead

Wake Technical Community College, Raleigh, NC

Nash Community College, Rocky Mount, NC

Southern Regional Technical College - Tifton (Formerly Moultrie Technical College), Tifton, GA

University of North Carolina at Charlotte, Charlotte, NC]

Our Employer Partners have played a big role in this grant. Each of the employer partners that are listed here are local to one of the schools, or more of the schools. Each of these grant partners signed on early when the grant was submitted and have been helping us along the way provide subject matter experts and provide resources. As we’ve gone, we’ve had other employer partners that have joined along with us as we’ve moved. To give an idea of the different types of industries, each of these folks are in, Clearwater Paper is a manufacturer of paper products, such as tissues, towels, and so forth. Duke Energy is a large power supplier in this area, in the southeast, and other parts of the country as well. Envirotrol is a systems integrator for HVAC services, and a lot of different critical areas where’s there’s manufacturing, whether it’s in data centers, whether it’s in hospitals. Heatcraft Refrigeration – they are an HVAC equipment manufacturer. Integrated Power Solutions is a contractor that does work in UPS systems, generators, power distribution work. Of course the Nash County Emergency Services and Police Department, their specialization is in emergency solutions, emergency preparedness, and disaster recovery. And of course that ties in with everything in the event of a natural disaster. And then STEAG Energy Services is a system that does chemical resources and chemical engineering for a lot of companies in the power sector.

Ncmo.us is the website for the consortium. There’s more information about this project, including our contact information, there. And hopefully more information will be put there as we go along, including the information and the links to the Skills Commons open educational resources. There’s links on there to take certification exams and also to sign up for classes.

With that I think I am going to turn it back over to Pam.

**Pam Frugoli:** Thank you Mitch that was very informative. I think we all learned a lot. It is always great for us here at DOL to hear about how the competency models are used in real life for really important purposes. The team here at the Employment and Training Administration helps to promote the use of the industry competency models for sector strategies and curriculum development at the state, regional and local level. And your example today shows that the models do serve as a common language around which the workforce system and education partners can engage with business to address workforce skill needs. And your application also illustrates how these national models can be customized for work in a state region or local area.

Mitch has already mentioned, and so I want to emphasize that the Cybersecurity Model that is posted on the Department of Labor’s Competency Model Clearinghouse website, the website is actually a representation in the pyramid format that we use for all of the competency models of a much more detailed model for cybersecurity competencies.

That model is from the National Initiative for Cybersecurity Education, also known as NICE, and the National Initiative for Cybersecurity Careers and Studies. So the link and home page is shown here in this slide for that more detailed model. If you in your own project are looking for additional details about cybersecurity roles, functions, and specific knowledge and skills--this is definitely the place to go. So we encourage you to take a look at it.

As Mitch has cited previously, this is the full Cyber Security Competency Model as it is displayed on the Competency Model Clearinghouse website sponsored by the Department of Labor. This tiered pyramid format is shared by all the industry competency models displayed on that site. Just to explain what a competency model is and why we chose this format:

A competency is: the capability to apply or use a set of related knowledge, skills, and abilities required to successfully perform “critical work functions” or tasks in a defined work setting.

A competency model is a collection of multiple competency domains that together describe the set of cross-cutting competencies required of workers within a specific sector of the economy. We would note that individuals in different roles or occupations within the sector will need to be able to perform at various levels of responsibility and proficiency on the competencies within that sector—but one of the purposes of the overall model is that all workers in that sector need to have at minimum an awareness and understanding of all of the competencies so that they can interact with their co-workers and people at different parts of the company or in different sections.

And then they also need proficiency in performing the competencies that fall within their specific occupational role—for example, some may perform an activity, others may supervise it, others may inspect it, or others may train on that activity.

In this way, each model provides an in-depth understanding of the field and highlights the cross-cutting competencies for careers in the sector by outlining the competencies in this structure of foundational tiers, which is the first 3 tiers, and industry-specific tires, which are tiers 4 and 5, highlighted in yellow on the pyramid.

As Mitch mentioned, cybersecurity has become an increasingly important field across many industries. The Automation model was recently updated in the past year. And as part of that update, an additional block was added on Tier 5 of the Automation Model called: Industrial Automation and Control Systems Cyber Security.

Note that in this slide we show that if you on the website mouse over a block, a blue block will appear that gives the title but also describes what that competency block is. And then if you actually click on the block you can see all of the content in the block. Finally if you want to see all of the model as a whole you can download the file with all of the content and I will show you that later.

So this is an example of the content you would see we’d clicked on that block. You see Critical Work Functions and Technical Content Areas. Note also that most of the statements begin with a verb. So they are competencies, things you need to be able to do. Sometimes there also is a list of relevant knowledge or content areas, or of specific concepts, terminology, or technology that workers would need to be familiar with to perform the competencies.

Each of the industry competency models have model champions. Many associations usually cooperate together and provide subject matter experts. But some of the lead ones volunteer to serve as champions for the models going forward once they are posted. These are the lead partners who contributed to the Automation and Cyber Security competency models. Industry model champions conduct outreach, notify DOL of examples of uses or applications of the model, and advise us about new resources that need to be added to the database. They also keep tabs on when an update to the model may be needed.

So for example, the Automation Federation is an association of member organizations engaged in manufacturing and process automation activities. Automation Federation provides industry-wide strategic analysis and coordination through its member organizations. In 2014 ETA worked with the Automation Federation and subject matter experts to update the Automation model to reflect the knowledge and skills needed by today's automation professionals. And as noted, it contains this new information on Cybersecurity in mission-critical operational technology, focusing on industrial automation and control systems. In addition, several key critical work functions in other competency blocks were modified to provide greater clarity.

And also, the National Initiative for Cybersecurity Education is a collection of more than 20 federal departments and agencies that collaborated to develop the cybersecurity workforce framework. And the DOL model incorporates competencies from that [National Cybersecurity Workforce Framework](http://niccs.us-cert.gov/research/draft-national-cybersecurity-workforce-framework-version-20) into the pyramid format shown earlier.

In addition, the DOL model complements that framework by adding the competencies needed by the average worker who uses the Internet or an organization's computer network, as well as by cybersecurity professionals. Workers on a network are often the frontline of defense against socially engineered cybersecurity threats that arrive, for example, via SPAM email and may introduce a virus into a network if a frontline worker opens an attachment, clicks on a website, or provides information to someone masquerading as a legitimate request. So we felt that providing the simplified competency model for cybersecurity on the DOL site would lead additional users to find the NICE framework.

This is another link that you can use to learn more about the NICE interagency collaboration and other work they are doing in addition to the cybersecurity workforce Framework that they have underway to promote a cybersavvy workforce and ensure that the U.S. has the trained cybersecurity professionals that are needed to keep all our mission critical operations and systems working

Earlier Mitch Sepaugh described how the project that he heads up used three different models in combination—Automation, Cybersecurity, and IT– to develop curriculum and credentials. On the Competency Model Clearinghouse website we have an infographic that you can download from the site under the Get Started tab that I will show you in just a moment. This infographic illustrates the primary user groups for the competency models—business, the workforce community, and educators. And it also provides an overview of different ways that the competency models can be used. So this can be a helpful handout if you are trying to get partners to collaborate with you.

So here I’m showing you the URL and the first page, the homepage, of the Competency Model Clearinghouse web site, which is a portal within the larger and comprehensive CareerOneStop website, all of which are sponsored by the U.S. Department of Labor. So, within the Competency Model Clearinghouse web site, there are 5 main sections. They appear as tabs in the upper banner: Get Started, Industry Models, Models in Action, Tools and Find Resources. We will take a look at each section of the website in turn. First I would like to highlight the industry models themselves.

Currently there are 26 different industry competency models on the DOL sponsored Competency Model Clearinghouse Website. Five new or updated models were launched in 2015. The Engineering model just launched in July—in partnership with the American Association of Engineering Societies, and many of the member associations who saw the need for a cross-cutting model for all of engineering, which can tend to become very specialized. They felt they were losing what makes a good engineer in general, and also they wanted to emphasize cross-cutting skills so that when engineers are laid off, for example when NASA downsized, they may have become so specialized that it is become difficult to transfer their skills if they have moved too far from the core competencies, even though they are very highly skilled workers. So the model helps to emphasize the transferable skills that all engineers possess.

And earlier in 2015 the following four models were launched: Hospitality, Tourism, and Events, which we collaborated with the Department of Commerce as well as industry associations on; a separate model for Food and Beverage Service; an Energy, Advanced Commercial Buildings model, which came to us through the Department of Energy; and finally, an Enterprise Security model. Note that Cybersecurity launched in 2014 in partnership with the Department of Homeland Security. Our Industry Competency Model team is currently working on updates to the Water Sector model, the Electronic Health Records, and the Allied Health competency models.

For those new to competency models and to the CMC website this Get Started section of the website provides all the background information and context. You’ll find here: a set of Frequently Asked Questions and answers; you’ll find User Guides; a description of the process of building a model; Tutorials on how to use online interactive tools, which I’ll mention later; guides on how to use and apply the competency models for a variety of purposes; and this is also where you can find the infographic and download it.

Tab 3 is the Models in Action Tab and Mitch gave us a great example, earlier, of how the competency models can be and are used. In addition to his example there are quite a few brief write-ups and summaries of different uses that can be found from this Models in Action page of the website. So these provides local examples of use for other models and for additional applications. You can find one perhaps that was already conducted in your own state or for an industry in which you are interested.

Tab 4 of the website is the tools. As mentioned previously, the competency models are national frameworks. Because it can be challenging to identify a representative national sample of employers in many sectors, what DOL does is convene industry associations that represent groups of businesses—along with leading educators and representatives of the workforce system and labor. When work on developing or customizing an industry competency model is done is at the state and local level it can be as a component of a larger sector strategy or economic development initiative.

Competency models can also be a great way to initiate engagement with business as workforce partners can reach out to them while already in possession of some information about the industry skill needs. So for example: You can ask them to review the model with workforce and education partners and customize it to fit their specific needs. This is so much better than arriving with a blank sheet of paper saying “tell us everything you need; businesses usually don’t have time for that!

For these reasons, this is why the CMC website provides interactive online tools to permit users to create customized versions of the competency models. Within this online tool, users can also save the models and return to them, work on them as a collaborative project with others, and save the final results in various formats. Users create a log-in account simply by submitting an e-mail and password and then they can select which model to use as a starting point. The tool then permits them to select which elements of the model to keep, which to omit. It further allows them to edit existing language, or to add to the language or add elements. There is also a tool to use the competency model to construct a visual graphic of a career ladder or lattice that may be being developed as part of a sector strategy or career pathway initiative. And Mitch, earlier, mentioned that his team used 3 different models in their work and we are close to launching a feature that will let you do that within the interactive tool. Currently you start with one model, but you will be able to pull in components from more than one model.

Finally Tab 5 is the Find Resources Tab. As part of the research that our team conducts to develop a first draft of an industry competency model, the team at DOL researches a range of resources including existing curriculum, certifications, industry studies or articles, bodies of knowledge, things like that. So all of those sources are entered into a database that is searchable in case other users want to refer to the original source material or want to find additional detail. If other resources are identified during the course of developing and validating the model, they are added to this database also. And finally after a model is released new resources are also added subsequently as new research or reports come out. This is one things that our industry champions make us aware of – materials that should be included or linked to.

I also want to point out that on the page where each industry model is displayed there is a link that allows you to download the model in various formats. These include a word version, a pdf version, as well as excel spreadsheets designed for a variety of purposes including: Identify Credential Competencies, Curriculum Analysis, Employer Analysis, or Gap Analysis. Users can also customize the column headings within these worksheets. But for example in the curriculum worksheet, you can put the courses within a program along the column headings and then the competencies are down the left hand side and you can check which competencies are covered in each course to make sure that all competencies are covered somewhere and that there’s no unnecessary duplication of material across the curriculum.

I just want to conclude with a slide that pulls together some of the important links that both Mitch and I have mentioned today, so you see them all in one place. And we thank you for listening and hope you find this information helpful and useful as you work to help build the cybersavvy workforce of the future!!! Our contact information is on the next slide—in case you need to find out any more specifics.

Thank you again.

<end>