THE BROOKINGS INSTITUTION
SAUL/ZILKHA ROOM

HOW TO IMPROVE CYBERSECURITY CAREER AND TECHNICAL EDUCATION

Washington, D.C.
Wednesday, March 13, 2019

PARTICIPANTS:

Welcome Remarks:

DARRELL WEST
Vice President and Director, Governance Studies
The Brookings Institution

Panel Discussion:

SUSAN HENNESSEY, Moderator
Senior Fellow, Governance Studies
Executive Editor, Lawfare
The Brookings Institution

THE HONORABLE JIM LANGEVIN (D-RI)
Co-Chair, Congressional Career and Technical Education Caucus
Co-Chair, Congressional Cybersecurity Caucus
U.S. House of Representatives

THE HONORABLE GLENN THOMPSON (R-PA)
Co-Chair, Congressional Career and Technical Education Caucus
U.S. House of Representatives

* * * * *

PROCEEDINGS

MR. WEST: Good afternoon. I'm Darrell West, vice president of Governance Studies, and director of the Center for Technology Innovation at the Brookings Institution.

And I would like to welcome you to our event on "How to Improve Cybersecurity Career and Technical Education."

We all know that cybersecurity represents one of the most important challenges of the digital era. There are malicious actors who've targeted governments, businesses and civil society seeking confidential information, or organizations and people who engage in outright disruption of digital networks.

To deal with these challenges we need to develop a critical infrastructure workforce that understands cybersecurity and can help protect assets that are vital to our society.

Today we are honored to have two very distinguished Members of Congress who are leaders on cybersecurity: first, Congressman Jim Langevin who serves on the Subcommittee on Cybersecurity and Infrastructure Protection. We actually met many years ago in Rhode Island when he entered public service, and I've been impressed at the amazing career that he has had since that point in time. Congressman Langevin also is co-chair of the Congressional Career and Technical Education Caucus, and also co-chair of the Congressional Cybersecurity Caucus. So, he is one of our nation's leading authorities on cybersecurity.

We also are very pleased to welcome Congressman Glenn Thompson from Pennsylvania. He serves on the Subcommittee on Higher Education and Workforce Training. He was one of the leaders who helped enable the Reauthorization of the Perkins Act on Technical Education. And so we applaud him for his great work on that issue. He also serves as co-chair of the Congressional Career and Technical Education Caucus.

So, each of the two members of Congress will make opening remarks outlining their thoughts on cybersecurity education.

Then we will have a moderated discussion led by my Brookings colleague, Susan Hennessey. Susan is a senior fellow in Governance Studies at Brookings, and also executive editor of the Lawfare national security blog. She also directs our New Cybersecurity Initiative, and is helping us think through both the policy and operational challenges in that area.

So, our first speaker will be Congressman Langevin. So I will turn it over to him. Thank you.

CONGRESSMAN LANGEVIN: Darrell, thank you very much for the introduction. It's an honor to be here today at Brookings. And I want to thank you all for hosting us, and to be with Susan as well. Thanks for moderating, Susan.

And it's a real thrill for me to be teaming up once again with my colleague, GT Thompson, from the great State of Pennsylvania, and he was really the leader and the force behind our collaboration on Reauthorizing the Perkins Act that modernized career and technical education at our high schools, and post-secondary programs. So, it's just an honor and a thrill to be teaming up with GT once again on this topic.

And I have some prepared remarks to just kind of frame the issue. And then I'll just get into the Q&A part of it. But this topic of cybersecurity and career and technical education means together two real passions of mine. Both of these interests came from distinct experiences that I had back in -- as a Member of Congress, back several years ago. Starting off in 2007, I chaired the Subcommittee on Homeland Security that had jurisdiction over cyber threats.

And I can remember my staff coming to me one day and telling me that I had to get a classified briefing about a significant vulnerability that two researchers out at Idaho National Labs had found to our electric grid.

And basically we arranged the briefing in secure space, and we started by talking about the issue, but then they showed a video of this diesel generator operating normally, and all of a sudden it starts spinning up beyond its capacity and started shaking, and basically as the seconds ticked by, ticked by, it wound up basically blowing itself up and -- because it had exceeded its capacity.

And what caused this was basically a simple piece of malicious code that was inserted into the generator's logic system. The Aurora Test, as it's now known, really opened my eyes to the physical damage that could be caused by a cyber incident, and subsequent lack of concern from the owners and operators of the electric grid, and safety of its delivery systems really it convinced me that Congress had a significant role to play to address this vulnerability, this problem.

A year later, on another topic, we were in one of the worst recessions in our nation's history and, 2007/2008, and as my constituents had really struggled with a dismal economy, I would, as I usually would go and tour businesses throughout my district, particularly in the manufacturing field, and I asked them, you know, almost afraid to ask. But do you know: when do you think you're going to feel confident enough that you're going to start hiring again?

And in my experience, especially in manufacturing facilities, that the answer I got time and again, we are actually hiring right now in many positions, but we are finding it a difficult challenge to find workers with the right skills to do the jobs that are available.

So, the skills gap really prompted me to look into policies that could bridge the gap between what the industry really needs and what our education system was teaching. And in this case I found that we already had a proven solution, that's CTE, Career and Technical Education.

So, ironically it takes me -- it took me really a decade now to bring these two issues together that I could work on jointly, but eventually after the countless speeches, where we exhorted people to take a fresh look at CTE. After all, advanced manufacturing jobs today don't at all resemble the manufacturing jobs of our parents and our grandparents, that we are the next generation, and I really started to wonder how much people, entering these exciting new companies, knew about cybersecurity and its importance.

And the answer that I found was, it was really very little, and it's not very surprising. So, we've long faced gap, if you will, in OT and IT, and that is, there's a difference in maturity between cybersecurity risk, postures of operational technology networks, which encompasses industrial control systems, or SCADA systems, and other systems that have real-world, physical impact and the information technology networks that have laptops, and tablets, and smartphones that we're more familiar with.

So cybersecurity awareness in the IT world has increased pretty dramatically, and a lot of companies that are now taking steps to educate their employees, whether through traditional training or more novel approaches like, making you aware of phishing emails.

But what really got my attention now is that we're far behind in the OT world, and part of the reason is historical, it's only in the last 10 to 15 years that OT systems started to be connected to the Internet, and therefore are now vulnerable.

So, these types of systems have -- they’ve brought great efficiencies to things like power plants or the electric grid, but with those connections, and to these OT systems down to the Internet in particular, if they're on the Internet, it brings great vulnerabilities.

And so part of this we found, and why it's not a high priority to security, is due to the gap in the skills training that GT and I are trying to attempt now to the -- by introducing the Cybersecurity Skills and Integration Act of this year, H.R. 1592, 1592.

So, basically in high risk, safety-critical sectors, where there's telecommunications, or manufacturing, or health care, a workforce without basic cybersecurity skills, in my opinion, can be very dangerous. And so we're trying to basically address these topics right now, close that gap, and we need to be successful.

So, you know, I just want to kind of wind up with this. And while it's important that we have certainly cybersecurity experts to help protect our different sectors, it's also important that at every -- that every worker, especially those dealing with OT, understand their role in keeping our systems secure. And this may be as simple as changing a username and a password, or reporting phishing attempts, but it's crucial for our Homeland Security.

And just by way of giving an example, you know, when you think of many fields, whether it's electricians, or other fields, they are steeped in this culture of physical safety. You'd never seen an electrician leave a door to a high-voltage distribution panel unlocked, for example, but you may never see he or she plug in -- they wouldn't think anything about -- they wouldn't at all walk away without closing that up, but you may see him or her, plug in a network cable and walk away, and not be conscious of that security, so that safety issue.

So, what's clear is that most cybersecurity experts I talk to with this, is that plugging in that smart device without changing the default credentials or learning the network team is inherently unsafe and we obviously need to -- we need to address this challenge, raise the awareness and the skills training, so that as they're being trained in this security and safety culture, that cybersecurity is a part of that.

So, that kind of frames where we are going, what we are trying to do. And I'll turn it back over to Susan or to GT. Thank you.

MS. HENNESSEY: Congressman Thompson?

CONGRESSMAN THOMPSON: Susan, thank you. Thank you, all of you for coming out today for this. I mean, this is a great turnout, and it is so important that, you know, we are paying attention to this issue. Thank you Darrell and Susan for your leadership, and facilitating here; and thanks to my friend, Jim, here, don't let -- you know, we've got a reputation, so don't let him know that we are working together so well. (Laughter)

We've always worked well together. Jim is just a dear friend of mine, and a colleague, and we've got a long history of legislative successes now for many years when it comes to skills-based education, when it comes to restoring rungs on the ladder of opportunity.

And so I'm really proud to be working with him. He brings the true -- in this particular partnership -- the true expertise in cybersecurity with his background and the things that he's worked on, so I've learned a lot from this man, and this is a great partnership for us.

You know, cybersecurity is something that impacts most Americans. I would say it impacts, today, every American, unless you live off the grid, no phone, you keep your money under your pillow, or under your mattress, that was probably the only exception where you potentially could not be impacted by a cybersecurity issue. It is that broad and that important of an issue.

It is the intersection of technology, of innovation, and quite frankly the need for efficiency in what we do, and workforce needs. It's all those things. And it also is a cross section of opportunity and risk. I used to love it that my -- you know, every so often there would be a new phone with new technology. It's hard to call them phones today because of everything they do.

Well they say there's more computing capability than in what those first astronauts that went to the moon. And I used to love that until after my son was wounded with an improvised explosive device in Iraq, and it became a stark reality that every time that I enjoyed a new function and feature on my cell phone that there was a terrorist using some of that technology to somehow more -- in an evil way, but an innovative way, detonate IEDs.

And so technology comes with -- it's an opportunity, but there is risk to manage. And that's what, that really is, probably the short definition of cybersecurity, with what we're doing. You know, and the average citizen needs to be aware of bad actors who would have obtained their sense of information, virus or spyware, you all know this.

I mean, it runs the gamut, cyber intrusion runs the gamut of privacy, just privacy issues which are so important today, of protecting our information, and there's so much available on the virtual highway today, so to speak, you know, to unethical business practices, you know, to cybercrimes, to cyber terrorism.

I mean that's just the world that we live in today, and I don't see that changing any time soon. You know, most citizens are utilizing the Internet for personal banking, and cyber commerce, and tele-education, and tele-health, and so, so much of our lives are streaming today. And so, you know, really those issues that we need to safeguard, and we need the workforce to do that.

So, let me cut to the chase. We need a workforce that understands cybersecurity at all levels, at absolutely all levels. We need men and women who have the skill sets to be leaders in security. I mean, you know, I wish the people, the individuals out there that would do cybercrimes, and cyber terrorism, compromising people's privacy, you know, exercising unethical business practices using cyber means, I wish they would use their energy and their knowledge for good. This world would be a whole lot better place.

But unfortunately, that kind of evil exists, and so that's why we need to make sure that we are encouraging and recruiting the best and the brightest when it comes to cybersecurity skills. That is our defense.

And it's not easy, because as you all know, it's redefined as technology changes, and improves, and it's used in different ways. So it’s really a battle, it's an effort that requires us to be proactive, to anticipate, and we get that with the number one asset in that effort is a qualified and trained workforce. There's no doubt about it.

You know even, I've been working in Career and Technical Education for more than a decade now, and last Congress we were able to pass a bill, and I was proud to lean on Jim's support as the original co-sponsor, and I was proud to be with the President on July 31st this past year when he signed the -- in the Oval Office -- the Strengthening Career & Technical Education for 21st Century Act.

Now the cool part about that bill is, you know, if you turn on cable news network all you see is division, and friction. And do you know, that bill was voted on six times between the House and the Senate, and in six votes not one person voted against it during the six times.

But we didn't see that reported on cable news network. I guess it wasn't newsworthy. I think it was, because I think it also, it shows how much -- and Jim and I have done some radio shows in the morning with C-SPAN, and we are used to the Republican line, the Democratic line, the Independent line, and it's like throwing -- and typically if you watch, it's like grenades going back and forth.

We are on. All people wanted to -- it doesn't matter what they registered, every line, it was just talking about how a career in technical education has made a difference in their lives.

CONGRESSMAN LANGEVIN: Yeah.

CONGRESSMAN THOMPSON: Or their children's lives, or their grandchildren's lives. And that's why -- and now that we're taking it to next step, which is really, you know, a lot of different ways, but particularly, and particularly today we are talking about cybersecurity and that skill.

So, yeah, there's more than 7 million jobs that are open and available and out there today, and certainly in one of the various threats or challenges, as Jim talked about, is the skills gap. But we've accomplished a great deal within the legislation that has now been signed by the President to not just reauthorize the Perkins Act, but to reform Career and Technical Education so that we are actually focused on restoring rungs on ladder of opportunity, and looking at in-demand positions.

And there's very few that are probably as in-demand going forward as cybersecurity, because it impacts every industry, every industry can be vulnerable.

And so, really, I'm proud to work with Jim, and on the most recent bill, as he mentioned, H.R. 1592, which is a Cybersecurity Skills Integration Act, a great, competitive grant program that does the kinds of things we are even working on, encouraging the partnership between employers and educators. You know, that public-private partnership to address in-demand skill sets.

And with more than 16 critical infrastructure sectors in the country, we really have to prepare our next generation of learners that they have the most sophisticated and compressive educational programs to project the Nation's dire assets, systems, or networks operational technology, those control systems that are part of almost every manufacturer today.

I mean we have fewer people working in manufacturing today, but it's because of technology, actually manufacturing is a larger part of our gross domestic product than any time in history. That's because of technology. So, this is about managing that opportunity, and the risk that comes together.

So, let me just close there. And I'm looking forward to your questions and discussions. And to just say once again, thank you for your interest in this, that is extremely important given the significance of cybersecurity, really, in all aspects of our lives.

MS. HENNESSEY: Thank you to both of the Congressmen for joining us here today. I like to start every cybersecurity panel by attempting to scare the audience a little bit. (Laughter)

CONGRESSMAN THOMPSON: That's easy.

MS. HENNESSEY: I think that here (inaudible) would agree that you are both facing overwhelming and urgent legislative agendas right now. It takes a lot to get congressional attention on a particular issue, and so I'm curious as you -- whenever you've introduced now, this Cybersecurity Education Integration Act, what are you concerned about? What is your fear if we don't have this kind of intervention? Sort of, what is the long-term landscape if we don't address these issues now? And I put that to both of you.

CONGRESSMAN LANGEVIN: Just yesterday we had a hearing on the safety and security at chemical facilities for example and, you know, I asked -- and then they talked about the safety training, the protocols that they have in place, and how their workforce needs to be, you know, part of the safety training so that, you know, they're doing the right things when they're managing these facilities and servicing the facilities, making sure they're running at optimal capacity.

And so I asked, so what type of cybersecurity training -- and this was the person who was directly responsible for representing the workforce -- and I asked: what type of cybersecurity training do they their workers get? And he said: I'm really not the cybersecurity expert so I really can't answer that question.

And that kind of goes to the heart of what I'm most concerned about. That's where the bad things can happen. I mean you'd be obviously worried about making sure that the physical systems couldn't release chemicals into the atmosphere, and that it's going to cause significant harm to not only the workers there but the surrounding population.

And what we are saying is that there are people that now service these -- not only need to be concerned about making sure that the valves are replaced, or that when they are -- before they went out that the safety systems are up to standard. But also now these remote systems, and OT systems, operational technology, that have sensors on them and such, and can be managed remotely that they are now -- they are now -- they have to be secured when they are serviced and they are installed.

Or the bad thing that could have happened before by some physical activity, like an explosion, or some physical hands-on sabotage, now it can be done, potentially, remotely so we want to make sure the people that are installing and servicing these systems, are cyber-conscious and cyber-trained.

CONGRESSMAN THOMPSON: I think it's comprehensive; just like Jim said, but it's the comprehensive concerns. I mean just last week I got an email on my personal email that said that, you've been hacked, send me USD100, and we won't do anything. And I'm thinking, well, you can hack my email and take a look at it, there's not much there to see, you know. You're not getting a hundred dollars.

You know, it's the cybercrimes like that, it's certainly unethical advantage that's taken, either by countries, by nations or by businesses, you know, in sort of cyber espionage. Yeah, you know, and it runs the course, cyber intrusion runs -- you know when you think of the critical infrastructures we have and I'm a -- I'll focus on, you mentioned manufacturing, let me focus on agriculture.

I was Vice Chair of the Agriculture Committee, a Senior Member on the Agriculture Committee, and when I look at our food processing, not only, food production as well, it's our farms are wired. I mean we are administering -- we are measuring soil health as the tractor runs over, and using a GPS device that doesn't really need to be driven, some of these tractors.

It's measuring soil health, and administering pesticides, insecticides, nutrients, and it's all done, basically, virtually. And so in processing plants where we are talking food, so how sensitive is temperature, you know, when it comes to making sure that there's no variance that we have not just high quality, affordable, but safe food.

And so the exposure, anywhere where we have this, this technology that is now online and vulnerable, you just take one of those, a transportation issue, a manufacturing issue, an agriculture issue, a defense issue, a financial services issue, that's the stuff that these novels are written about actually, you know.

MS. HENNESSEY: That was even scarier answers than I had expected there would give me. So, thank you --

CONGRESSMAN THOMPSON: Sorry about that. Welcome to our world.

CONGRESSMAN LANGEVIN: Yeah. That's right.

MS. HENNESSEY: Moving to sort of the specific legislation, Congressman Langevin. What is the goal of this particular piece of legislation? What are you hoping to accomplish with it?

CONGRESSMAN LANGEVIN: So, we want to create -- again, I believe heavily in, and GT does as well, on the public-private partnership, and so the whole goal of the Perkins Reauthorization Act is to make sure that there was better alignment between what we are teaching in our classrooms and what our real-world needs are in business.

It's that Perkins hadn't been reauthorized for ten years, and so we teamed up to bring that reauthorization through Congress, and so it ensures closer alignment between what we are teaching in schools and what businesses need, and it ensures that businesses, obviously, have a seat at the table.

What we want to do in this, with the New Cybersecurity Skills Training Act is to make sure that that we develop curriculum so that our people in these -- in these CTE fields that are dealing with safety systems, and such, and dealing with OT systems are properly trained.

Right now the programs don't really exist, and so would be focused on a grant program creating demonstration programs that would create curriculum where there's a partnership between academia and businesses. So it would be encouraging that kind of collaboration, would be a $10 billion authorization to develop the programs, and they would be taught at the post-secondary level.

And the goal of course would be that eventually, once the curriculum is developed, that the curriculum would eventually migrate down and be used at the secondary school program level as the kids are getting trained. But these people right now that where we are focusing on at first, a place like the CCRI, Community College of Rhode Island, teaming up with an electric boat, for example.

They are training people to go into the field of building submarines, on submarines they're going to have sensors attached to monitoring safety systems and such. We want to make sure they, or again similar fields, that they're trained also in cybersecurity, so that as they are installing sensors, that they're going to actually be safety, both virtually and -- there will be safety and focused in both the systems and the programs that they're connecting.

MS. HENNESSEY: Congressman Thompson, I'm hoping you can sort of walk us through how the bill operates, right? So, if you are planning on changing university behavior, how does it work?

CONGRESSMAN THOMPSON: Sure. Well, first of all let me just say when you think of Career and Technical Education, it's not necessarily -- we are probably not talking about a 4-year degree. It's not to say that somebody won't eventually -- I look at it this way, if I'm going to hire an engineer, I think the best possible engineer I could hire is somebody who, perhaps even at a secondary level, had gotten some skills-based education in welding, and draftsmanship.

And they have those basic skills and they understand how things get built, they are going to make an amazing engineer after they go on. So, it's kind of a ladder of opportunity to be able to climb. And so there's no one particular place for this, it could be a career and technical education school; it could be empowering an employer who has cybersecurity needs.

We put, within the Perkins reauthorization that we did that was, again signed in July into law, you know, we really built some strong -- returning to a strong, robust apprenticeship program that -- where the employers are really at the table there. We are trying to bring the people who sign the front of a paycheck, not the back of a paycheck, to the table, so that we actually educate to the needs.

And we are also providing ability to pivot for those educational institutions. You know before, you could have an emerging need in your community, maybe it's somebody who grew up in one of our congressional districts, we could cite a number of examples of those, yeah, and they wanted to come back home. Because they had gone off and done great things, they created these big businesses, with probably thousands if not hundreds of jobs and they -- and they wanted to come back, and they want to build a business, and I've seen examples of this.

And then do you what their number one need is? It's a qualified, trained workforce. And so they do reach out to our educational institutions and they'd say, do you know what, I'll create 500 jobs if I can find the qualified and trained employees.

Well before our law got signed, trying to -- I mean to get approvals for starting a new program that was at the speed of bureaucracy. You know, it would be sometimes years until -- it's like turning an aircraft carrier in a typhoon. You know, it usually doesn't work.

But now this, under the underlying law that we started with we created the ability to pivot, so that that foundation will be very helpful for what we are working on now with cybersecurity, because the demand is there, it's obvious.

And now communities, whether it's community colleges, career and technical education, business, industries all sizes, that want to do apprenticeship, do their own training programs will now have the ability to step -- you know, kind of step up those programs.

MS. HENNESSEY: So, Congressman Langevin, are there examples of programs or universities that are already doing this well, or is this sort of uncharted territory, and where you're trying something that's sort of wholly new?

CONGRESSMAN LANGEVIN: Yeah. So, in a lot of ways it's uncharted, but we look at NIST, for example, this is the program that we would use as a kind of foundation, the NIST, it's the NICE framework, it stands for the National Initiative for Cybersecurity Education. And basically it would use this as a model, as the foundation to build a program going forward.

But it puts real context to what the need is out there, and as curriculums developed, and they're doing career and technical education development programs that we incorporate that that cyber element in it. So NIST is where we look as the primary resource as the programs develop, but there is a model that we would we would start with.

CONGRESSMAN THOMPSON: And our district lines were redrawn by some judges -- that's a whole another section we can talk about -- this past year. But before that I had the privilege of working -- representing in Erie County a university -- a small college actually -- and they had two campuses that they actually get into workforce development, not just the traditional four-year path.

And we've got the Tom Ridge Cybersecurity School there, and so they were really cutting new ground, recognizing the need for that skill set.

But I would argue if you look at some, in even our traditional career and technical education programs, and that's the beauty of Career and Technical Education, the tools of Career and Technical Education is, you know, it's the things people normally think about, it's welders, and hammers, and wrenches; but it's also paintbrushes, and scissors, and stethoscopes, and keyboards, and industrial control systems, and operational technology applications.

I mean it's just so varied that I mean if you go into a heating, ventilation, air conditioning program with high school kids today they're working with controls that are wireless. I mean almost -- you know many of the traditional programs out there, you know, this technology and innovation is being innovated for efficiency purposes, and convenience to the consumer into those programs.

And so those kids will say, and then adults, because Career and Technical Education is for everybody at any age, we envision that as a portal, you go in and get what you need, you come out and get a better job, you get a raise to better support your family. You know, those skill sets also have to not just have the skill to deal with the opportunity, but we need to educate them to the risk.

MS. HENNESSEY: This is sort of framed as a pilot program, I assume that means that if it works it will be expanded. How do you think about measuring success? How will you know if this program has worked?

CONGRESSMAN THOMPSON: Well, a part of it is witnessing it. You know, it's expecting to look for those reports back, or lean heavily on the Department of Labor, and on the Department of Education to -- you know, for the Department of Commerce. You know, they should all be monitoring with this concern.

And actually, quite frankly, the Department Homeland Security ought to be looking at this as well, because of the cybersecurity threat. So, our expectations I think would be that -- you know, that it's implemented. And then I learned a long time ago, it's not sufficient just to write and successfully get what I think is righteous legislation signed by the President, but I don't ever trust turning it over to unelected bureaucrats without some oversight.

You know, I've seen situations where, well, and one of my first bills dealt with telemedicine, and how the Department of Defense completely misinterpreted what my thoughts of telemedicine were. They stepped back. They called me up one day and they said, Congressman you're going to love this. We are fully implemented; we are going to be able to save lives because we are going to provide more access to health care through telemedicine, for Active Duty, Military, Reserve and Guard.

They said, this is perfect, all these soldiers need to do is show up at a fort or an installation and we'll hook them up with telemedicine. And I'm thinking, you people missed the boat. (Laughter) I want them to be able to do that when they're depressed at their dining room table.

And do you know what? And do you know what? And that oversight made a difference. So I think that's part of it, it makes it when we're done with this we're not going to be done with it. We have to provide oversight, and hopefully we can have, you know, the future goal which would be great, but to have hearings, you know, to provide some transparency on how things are going.

Have people coming in to witness, you know: what difference has this made for an industry? What difference has this made for somebody for, you know, a better life opportunity?

CONGRESSMAN LANGEVIN: Right. I think that oversight is exactly right, and we'll follow up on this making sure that -- I guess I will look and say, in addition to the oversight, looking at, if the NIST framework standards are adopted throughout the CTE training programs, where there's any type of IT or OT training that's involved.

So we, GT and I, we teamed up on modernizing the Career and Technical

Education programs and again whether it's in advanced manufacturing, working with robotics, whether it's plumbing and pipe fitting, and so those have been -- we are going to make sure those are modernized and up to what industry needs, but then anything that touches also on an IT or OT training that, again, cybersecurity is built into it.

I think we are all becoming more and more aware of the fact that we are part of the solution when it comes to dealing with IT, and most people know that: okay, you should have a strong password in your system, you should have malware protection on your computers, that you're downloading your security patches, don't click on unknown links or download -- you know opening up attachments that are sent to you by an unknown source.

You know, basically a high percentage of the vulnerabilities and in cyberspace can be addressed by practicing good cyber hygiene, and so now we are also addressing the gap in not just IT security but in OT security.

So, these systems that that caused a physical action that, again, used to be done kind of just locally, now are managed remotely, so opening up or closing valves, causing a generator now to kind of spin up or spin down, depending on the load that's needed, these OT systems are now connected and networked in a lot of ways.

Hopefully they're not necessarily always connected to the Internet, but they're going to be connecting to something, and allowance for that -- the remote management we want to make sure that the people that are installing and servicing these systems, have cybersecurity as a forethought and not just an afterthought.

MS. HENNESSEY: I'm curious. Why do you think that the private sector isn't getting this right on their own? Right? These companies are going to be sort of the OT sector, they are the ones who bear the immediate cost of sort of a cybersecurity event. And so why is it that you think that we aren't seeing sort of that prioritization, you know, of cybersecurity in that field?

CONGRESSMAN LANGEVIN: A lot of is because the curriculum doesn't really exist, and it hasn't been a focus, that's why we're saying that we are going to make this a priority. We are going to we're going to work with industry, in academia, to develop these pilot programs and the pilot training, and make sure that that curriculum is incorporated.

You know sometimes also there's this hope, I believe, maybe it's not going to happen to us. And that's one of the things I found at the electric grid, for example, that there was a sense that, you know, where, we've got this, and we've installed, we have strong cybersecurity measures in place. But when you peel back the onion though, we found that that's not really accurate.

Now it's getting a lot better than where it was back when I first started on this field of cybersecurity, but it's a work in progress and as, you know, technology changes and improves we need to -- we need to keep up with the changes, and keep up with the threats.

And we're also looking at, again, closer partnerships between critical infrastructure and Department of Homeland Security. All these things are a work in progress. We are getting to a better place but it's, you know, we can't rest on our laurels either.

CONGRESSMAN THOMPSON: Now you need workforce, I mean that's -- I think you'd be hard-pressed to find anyone who, in any of the industries we've mentioned who are not -- I mean that are not successful knowing that the cybersecurity concerns has to do with something that they're talking about.

And, you know, quite frankly they need a qualified and trained workforce, and so this -- and it's a fairly recent advent when you think about it, in terms of something that's a decade or decades-long in terms of development, but it's certainly a part of almost every -- I can't think of too many industries that wouldn't be impacted today.

MS. HENNESSEY: So you've mentioned sort of the number of sectors that this bears on, everything from agriculture, to health, to defense, your bill uses the DHS definition of critical infrastructure. One sort of critique of that definition as it relates to DHS is that it encompasses so much that if everything is critical nothing is critical. And so as you start to approach these issues as a matter of congressional priority in a world of sort of limited resources, how do you think about defining that sector, you know, for that prioritized attention?

CONGRESSMAN THOMPSON: Well, I don't think you can limit it, because there are so many vulnerabilities today, I mean sadly -- I mean I'm sitting here with two cell phones, and mobile emails, and all the stuff that go with it in my pocket today, not my choice, but by necessity, because that's the way the world is today. And so it's overwhelming from the perspective that you described, that there are so many sectors that would be a part of this. Sixteen, I think, perhaps officially is a number that comes to mind.

But what is the common thread? What is the common thread on this? The common thread is having someone who is available that is qualified and trained, that anyone and any industry, whether it's those 16 or others, could go out and recruit.

I mean the good -- the great news of this is, these are great jobs. The bad news is, we don't have enough warm bodies for all the great jobs, so that's kind of, you know, something we need to work on as well

CONGRESSMAN LANGEVIN: But GT mentioned that, you know, the Department of Homeland Security it's their definitions, they have the 16 sectors that they would define as critical infrastructure. That's where, you know, we are going to -- we are going to focus on first. But look! We need to make sure that there are relevant skills, 21st Century skills for a 21st Century economy.

And, you know, as other sectors obviously are created, maybe they don't even exist today, what I've been thinking about, that we are adaptable, and we are making sure that the this curriculum, and it deals with anything that might be considered critical infrastructure, and IT, and operational technology connected, that we are adaptable. And as I said, that's forethought rather than an afterthought, as I said.

MS. HENNESSEY: Congress Langevin, can you, as the Co-Chair of the

Congressional Cybersecurity Caucus, I'm wondering if you can speak to some of the challenges of educating your fellow members on the nature of the issues here, and the urgency of the problem?

CONGRESSMAN LANGEVIN: Yeah. So, again it's constant work and effort to just you know continue to raise these issues. And, you know, GT and I use our respective positions as Co-Chairs, now the Career and Technical Education and Caucus, and I have a Republican colleague, Mike McCaul he and I created the Cybersecurity Caucus together, and we use these forms as an opportunity to educate members and staff about the -- you know, the issues in these areas.

And so we hold briefings, and sometimes it's government experts, sometimes it's industry experts, or people from academia, but the caucus is just an opportunity, provide a forum for education of members and staff, and that's what we'll continue to do in this particular issue as well.

Again, it's one of those things if we were silent on it, you know, then who is paying attention to it, but this is an area of interest for GT and I, and so we want to bring the relative, the next relative -- relevant experts into the process to make sure we are educating members and staff.

I used to get a lot of funny looks, you know, 10 years when I started talking about cybersecurity and the damage that could been done, and I felt, like with those little guys with the tin hats running around, that the sky is falling. You know, now everybody gets the importance of cybersecurity, and so we are going to use our positions to persist and (crosstalk)--

CONGRESSMAN LANGEVIN: Persistence is important on public policy. I mean there are a lot of fly-by-night things that happen just off-the-cuff, and usually it's not the best legislation, it's more emotional than science and data based and -- but I find that, and this falls into that category, you know, you have to be persistent.

We've been working -- we worked on that Perkins Reauthorization literally for 10 years, and sadly it took 10 years, so we came really close the past couple -- but close doesn't count unless you're playing horseshoes, and so we finally got it done in the 115th Congress. But you've got to be persistent especially on the things that are important

MS. HENNESSEY: So you've mentioned a little bit about the focus on the polarized nature of Congress. I'm curious. For both of you, how do you think about bipartisanship and sort of its role in cybersecurity education?

CONGRESSMAN THOMPSON: It's incredibly important. That's the only way we really get things done that last, and that are sustainable as well when we do in a bipartisan way. And no single party has got a corner on the best ideas, you know, you need to be of willingness to -- and I think that Career and Technical Education Caucus actually has been a great example that.

You know, we want -- we invite, we encourage, not just our colleagues in both parties, but we, well we engage students, we engage employers, we engage folks that are doing the -- offering the education, skills-based education to the table. And I think that is incredibly important with this, so we bring everybody to the table, and then we see what we can agree upon.

And I that's basically what we did on this, on the framework of this -- and I know it's just a pilot but it's incredibly important with the cybersecurity. And so that's -- I mean that's my perspective one it anyways.

CONGRESSMAN LANGEVIN: Yeah. And I'll just say, you know, if all you're doing is getting your information by watching the, you know, the high-level things that they're talking about and in the news media can be pretty depressing, and you think about the polarization in the country. And I don't -- you know, I didn't discount that, that there is a -- that the country is divided in ways, and as is, you know, the Congress.

But there are a lot of areas where we find agreement, and I think by focusing on, you know, things that really matter to the folks back home, you know, bread-and-butter issues, and this is really a bread-and-butter issue as far as I'm concerned, job training, workforce development. There is bipartisan agreement and, you know, I believe that it starts with us as Members of Congress, that we've got to, you know, work at it, be conscious, of reaching out across the aisle, finding those areas where we can work together.

And certainly GT and I do that. That's one of the real moments of pride that I have in my years in Congress, and talking about accomplishments, and how we're making a difference in helping people that are in our respective districts. I mean my partnership with GT has been one of those real highlights that I'm proud to talk about, always.

CONGRESSMAN THOMPSON: And then to recognize, we are not always going to agree too. That's the beauty of the legislative process is that we are a diverse nation, and we should celebrate that diversity in those -- and get all that diversity to the table of ideas, and who we are, and I do like to tell people, there are some folks out there that talk with me and they're just absolutely convinced that that friction is an absolute bad thing in Congress, and that we should always agree.

And I looked, usually look at them and say: you know, if you think that we should agree all the time on everything, you probably have never been married. (Laughter) Because life just doesn't work that way. You know, you don't always get everything you want, you know. You’ve got to work together. Right, yeah?

CONGRESSMAN LANGEVIN: Mm-hmm. That's right.

MS. HENNESSEY: I think we have some time for some audience questions; and if you raise your hand and wait for the microphone to come to you. I guess, Moderator's privilege to please ask, that it be an actual question.

MR. NELSON: I'm Mike Nelson. I used to teach Internet Studies at Georgetown. I really commend the work that you're doing here to solve one piece of the problem. There are really three market failures. You're dealing with the need for more cybersecurity experts, but last year we had 15 billion records compromised, and 63 percent of the time it wasn't an insider threat or a malicious hacker, it was insider idiocy.

CONGRESSMAN THOMPSON: Yeah.

MR. NELSON: Somebody did something wrong --

CONGRESSMAN THOMPSON: And (crosstalk)

MR. NELSON: So, those two problems, getting the people who run these systems, who often aren't trained in computer science let alone computer security, more aware of the threat. And the other market failure is getting the IT industry to design things that are easier to use. A lot of people in the field actually want things to be more complicated so you have to pay them more for consulting. Do you have any solutions to these other two problems, particularly, the ease of use problem?

CONGRESSMAN THOMPSON: I don't, but I'm sure Jim does. (Laughter) Any thoughts?

CONGRESSMAN LANGEVIN: Yeah. I mean, sure, ease of use is, you know, it comes in the design, right? And, you know, that is one of the areas where, you know, America shines really, and it's in our innovation, and making things easy to use. And by the way, so another passion of mine is STEM to STEAM, so bringing art and design into the science technology, engineering and mathematics --

CONGRESSMAN THOMPSON: And agriculture, it's (crosstalk). (Laughter)

CONGRESSMAN LANGEVIN: All right, and agriculture. You know, I use by the way the -- when I use the STEM to STEAM example I think about MP3 players, you know, really who the heck used them really as widely, until the iPhone came along. And there's an example of how you had, you know, art and design, incorporated in technology, just a vivid example of U.S. innovation.

So, that made technology, if you will, you know, more user-friendly, and easy to use. So I guess we have to, you know, be conscious of including user friendliness into design.

The other thing I will say on this in terms of baking security in, backing up more, and as we are developing technology we have security as a forethought and not an afterthought. And also, have a mechanism for closing vulnerabilities, say, after a product is developed. We are doing that in the post-secondary -- post-market guidance on medical devices.

And there was recently, you know, an agreement reached with the FDA and manufacturers, basically, that as long as you have those mechanisms in place, you know, you avoid the necessary costly things, like recalls, or other things that can cause problems. And it and it makes it more difficult, you know, after the fact that if it's both security is built in from the design phase early on as programs are being written and developed, and then also have a way of upgrading afterward that calls for security and safety all incorporated; so, being proactive and not just, you know, reactive.

CONGRESSMAN THOMPSON: And I think the competency of the workforce is part of it too. I mean obviously we're talking Career and Technical Education, but we need in our professional -- you know, beyond Career and Technical Education, you know, we need to equip a workforce of engineers, the people that can that maybe can help us deal that we don't have those incompetency issues that you referenced. And, you know, and to be able to -- it's always going to be a challenge too.

When I practice health care, I mean at that point technology was changing once every seven years, now it feels like it's once every seven days and so -- but having a -- really employing a qualified and trained workforce, so to be highly competent, you know, to be able to be our troubleshooters to, you know, to help us on those issues.

I know a lot of us, you're not going to -- not going to deal with all the problems that you’ve talked completely, but to some degree the better we do in workforce preparation, not just qualified and trained, but highly competent and effective could help us, give us tools we need.

MS. CULP: Good afternoon. Thank you for your presence and a very informative panel. I'm Margaret Culp; I'm an Independent Consultant, Retired Air Force, worked in Aircraft Maintenance. And I've interfaced -- one of the areas that I work on is National Service, and I've worked with the Academic Centers of Excellence both at the university level and at the community college, technical school level.

And there is a video from Israel showing that Israel has gone from pretty nondescript in the cybersecurity area to being one of the top five, and they use the rationale that they've had the National Service Program and that has been able -- enabled them to capture the best talent in this area.

Would it be an opportunity for our Nation, on a bipartisan level, to have national service that would include cybersecurity and other areas for our young people?

CONGRESSMAN THOMPSON: I think those opportunities within what we do now with National Service, AmeriCorps and others, you know, we ought to be looking at in-demand positions as we deploy people into different types of business, industries, agencies, and so, you know, this seems like -- again, unless you're someone who's going to live off the grid, and keep your money under your mattress, and not have a phone or any connection, cybersecurity is going to be a concern of yours at one time or another.

And I think it needs to be a part of our -- we need to look for those types of opportunities as we incentivize various types of education that, you know, it's a highly critical skill. And let's not -- I mean we really haven't talked about, or the fact we need to -- this is something that it would be great if the states would integrate into their curriculum for secondary school, elementary and secondary schools.

I mean the people that hack my phones more often than anyone else are my three and six-year-old grandsons. It's amazing how they figure out passwords, and FaceTime, and Twitter, and everything else. It's scary actually. I make sure I hide my phones from them, but these kids are sponges, right, at that age. And so if we could start to talk about this as a critical skill set for every American, and start actually in our elementary schools with it.

MS. HENNESSEY: I think we have time for maybe one or two more questions. I see a hand there, the green shirt, right in the back. Thank you.

MS. ROSETT-HAUBNER: Hi. Good afternoon. I'm Nikki Rosett-Haubner, I'm a School Counselor and Department Chair at Marshall Governor STEM and CTE Academy, just across in Tysons Corner, it's a secondary school. So we have a robust IT program, over 250 students who would like to take some sort of IT class next year, and we follow kind of along the CompTIA sequence, anywhere from A+ to Security+ training these students, we were actually named a Cybersecurity Center of Excellence by the Air Force Association.

But our biggest challenge is finding teachers qualified to be able to teach these students. I mean to have the content knowledge, and then those that are able to inspire students to pursue these types of careers. So, I was just curious if there's any -- if you guys address that at all in your most recent bills or legislation.

And then additionally, the funding for setting up some of these highly-specialized technical labs for the students to be able to have a safe space to learn cybersecurity without unleashing them on the worldwide web. So, those are the two pieces that I'm just curious if it's addressed in any place.

CONGRESSMAN THOMPSON: Well, Career and Technical Education, in general, one of the issues is finding individuals with the passion to be able to teach, to have that gift of teaching, because I mean, kind of the sad fact is that, you know, a lot of -- these are in-demand positions so sometimes what we pay our instructors is nowhere close to what they can make working in the private sector, you know, practicing their trade, their skill, their profession.

And so that is a challenge. Now, I don't think we -- I don't think we directly, but we do indirectly address this because this pilot programming is partnerships between industry and education, you know, employers and educators. And so, you know, there are a lot of times -- let's think about this: you know, who are the people that have the most at risk here? It's the employers. Right? It's the business and the industries that absolutely need this workforce in order for them to be successful.

I mean, this is a cost of their business, their reputation, the cybersecurity issues, all the things that can happen. And so the best -- well, the coolest models I've seen, I haven't seen in cybersecurity yet, okay, because we're just kind of at the cutting edge there, but I've seen it with other industries where employers will lend their -- put on, you know, will place their best employees in these education settings as adjunct faculty members.

You know, not even -- and at no cost to the schools, and sometimes if they're smart they'll lend lab equipment, or the types of equipment as well, and we certainly encourage that within what we put into the into the Perkins Reauthorization. So, you know, there is -- and Perkins does, as you know, and thank you for your -- it sounds like your school is closer, maybe if someone -- it's one we could come visit here sometime. That would be great.

But with the Perkins monies you can invest in different types of Technology, specifically your programs, there are dollars that are there as well.

CONGRESSMAN LANGEVIN: So, I'll say that, you know, cybersecurity is an example of that lag between what we're teaching in academia and what businesses need. There are over a-quarter-million jobs right now that go unfilled every day in the cybersecurity field because people don't have the right skills to do those jobs. And that's how we are going to grow exponentially as time goes on if we don't address this gap.

So, right now academia is catching up with cybersecurity. I mean up until, you know, not too long ago there wasn't even a program in the field of cybersecurity training, and so it started out with Certificate Programs, and then a Master's Program, and now it's being created that there's both minors and majors in cybersecurity, but it took time for these programs to really be developed. Because, you know, again the need was there but there was a lag.

So, as people go through these programs and get the skills, I mean the academic credentialing and training then there will, hopefully, be more people in the workforce that will also be willing to -- now to teach these skills. But you know it is a -- we're still sort of playing catch-up, but we will get there. This particular act doesn't necessary, per se, develop, address that specifically, but it will have the ancillary positive effects.

So thanks for -- you know, for raising it, but again, we need to continue to develop the workforce, to get all the policies and procedures in place so that we can pass the laws creating things, but you don't have the people to actually implement them and do the job. You know that's a -- that's a real problem and a challenge that we need to address it as well.

MS. HENNESSEY: Congressman Thomas, and Congressman Langevin, thanks so much for joining us today.

CONGRESSMAN THOMPSON: Thank you. Appreciate it. (Applause)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text under my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020