TechWerx State of Industrial Control System Cyber Security Training Opportunity Webinar Transcripts
11/19/2024

Meghan Camello, TechWerx:
Good afternoon and good morning, everyone, depending on when you're watching this webinar. We are very excited to host this informational webinar on a new TechWerx opportunity. This opportunity is called the State of Industrial Control System Cyber Security Training. This opportunity is being funded by CESER, or the Office of Cybersecurity, Energy Security and Emergency Response at the Department of Energy (DOE).

A quick intro. My name is Meg Camello, and I am part of the TechWerx Hub. TechWerx is a new innovation hub managed by RTI International in support of the Department of Energy. Our goal at TechWerx is to facilitate connections among federal, academia, nonprofits, and small businesses across the United States. To hear about any new TechWerx opportunities that come up or updates on this opportunity, we recommend you following our Linkedin page, as well as signing up for our newsletter on our website.

For this opportunity we will be hosting office hours. These office hours will take place December 11th from 2 to 3p.m. Eastern Standard Time, and during this session we will answer any questions that you may have about this opportunity.

Today we have joining us from CESER, Dr. Cynthia Hsu, who is the cybersecurity workforce program manager for CESER. Cynthia is accompanied by Fania Berwick and Dr. Kate McGrath.

With that I'll pass it over to Cynthia to cover more on the opportunity.

Cynthia Hsu, DOE CESER:
Great. Thank you, Meg. We're really excited to be sharing this with you and the work that we're going to present in front of you, and hopefully you will be excited about joining us and helping us to complete this work! Let me just have Fania come on and introduce herself very quickly. Fania.

Fania Barwick, DOE CESER:
Hi, everyone. I am the implementation manager for this workforce program. I am working with Cynthia, Kate, and Steve to help move all the pieces through the process and design the funding and the opportunities that we are putting out.

Cynthia Hsu, DOE CESER:
Great! And very critical lately has been Kate McGrath. Kate, you want to say hello?

Kate McGrath, DOE CESER:

Hi Everybody! Nice to see you all here. Thanks for watching. I'm really happy to be a part of the team working on this great opportunity. So, thanks for tuning in.

Cynthia Hsu, DOE CESER:
And Steve isn't with us today, but if you are one of the one of the providers and performers that we end up working with in the future, you will end up working with all 4 of us off and on. So, I think it's important always for you to meet the team that you might be working with, because I think we're pretty awesome. We're small and scrappy, as they say.

So, with that, let's just start off with why we're here, and I'll give you a few minutes to read this slide. But, the issues that we're facing in cybersecurity across the critical infrastructures, energy being one of them-- and I am partial to the energy one, because I work at CESER-- but these are not issues that are going to happen, or that we're afraid of happening. This is a quote from the ODNI report that comes out every year, and it's about what China is capable of now. And this is a report that is available to you in the public sector. So, this is not a security clearance report.

And the fact that the industry and the government are willing to put into words that this kind of challenge that we are facing from overseas actors is at the stage where it's happening is really important to recognize, because we're not talking about what might happen. There's a similar comment about what Russia is capable of, and there's a link here to the ODNI report, the office director of National Intelligence, and about what North Korea is capable of in the cyber domain, and what Iran is capable of in the cyber domain.

So, we are looking forward to working with you to help us improve the capacity and the skills of the energy sector cybersecurity workforce to address these threats and the threats that are coming at us in the future.

CESER has a great mission. The cybersecurity, energy security, and emergency response office that I work in cover everything from R&D to work like this, e.g., how do we improve the workforce? And today we're specifically here to talk about an opportunity that we're providing so that you can help us do two things. The cybersecurity workforce challenges are very broad, they cover a wide spectrum of things, and this particular opportunity we're presenting is focused on two spaces of that broader area.

One is how do we make decisions about spending federal funding and investing in workforce initiatives that will improve the capabilities of the incumbent workforce (so, people who are already employed in the energy sector). The second is, what can we do to increase the pool of potential employees that want to work in the energy sector in cybersecurity. That covers a lot and we have tried to scope this opportunity down so that it's more focused.

There are 2 pieces that are really essential here. One is, we're not talking about cybersecurity writ large. So, there's a lot of activity and training and courses in information

technology, cybersecurity. But we are focused very specifically on a subset called industrial control systems and/or operational technology cyber security (ICS/OT). ICS/OT cybersecurity has some overlap with information technology, but it has got some very unique aspects to it. So, we are scoping down this opportunity to really focus in on just the cybersecurity ICS/OT cybersecurity challenges that requires a knowledge of cyber security writ large, but it also requires knowledge and understanding of operational systems and engineering of physical systems. So, some of you might be familiar with the concept of CPS, cyber physical systems. These are digital systems that are digitally controlled, that result in physical actions and that's part of what separates it from general information technology. So, in that there's a lot of unique challenges in the ICS workforce and in it generally. But certainly in ICS. There aren't really standardized job titles and tasks and skills. So it becomes very hard to wrap our heads around. Who's doing what and how do you find out? What are the basic skills that are needed to work in ICS cyber?

It's also a relatively new profession, even newer than information technology. So, if you go to a bank and you apply. You probably won't. You work in ICS cyber. You're probably not going to see what's your job role. You're not going to even see that as an option, you might not even see cybersecurity as an option, because those institutionalized infrastructures don't necessarily recognize cybersecurity as a unique range of professions.

In addition, while we hear a lot that there are IT cyber workforce shortages. We have really no idea whether the energy sector is facing a shortage in the ICS cyber workforce. Anecdotally, everything we hear says, yes, but when it comes to data, almost all of the data that I've seen so far, is IT centric and isn't really focused on ICS.

So, this effort is really to drill down and look at what data we might be able to collect out there to help us understand what the ICS cyber workforce, again, narrowed down to just the energy sector, looks like. One of the other challenges is, you see a lot of entry level job positions posted in ICS cybersecurity and they're not very well aligned with what an entry level candidate might have in terms of knowledge, skills and abilities or KSAs. So, for example, I saw a job description in energy that asked for 5 years of experience implementing a new cyber security standard and that new cybersecurity standard had only been in existence for 2 years. So, already, it's not possible to fill that job because nobody has 5 years of experience with that standard. So, there's a lot of misalignment between what we're asking for and that gets back to the 1st bullet of how do we describe the tasks and the skills that we need for this workforce and then what the entry level or the pool of candidates actually has in terms of skills to apply for those jobs.

ICS responsibilities are also not clearly defined as an ICS job role. So, in order to collect this kind of data, you're looking around the edges. You might be looking at an engineering job description that has ICS as a subsumed under that. And so, it's not straightforward to do the kinds of data collection that you might be able to do for more established job roles. And that's what makes this all challenging and that's why we are reaching out to all of you

for help, because this is not something that's easily to wrap our heads around to create the kind of data set that we need to inform our investments in this area.

So, this opportunity is to support market research to understand what the landscape is who is doing training and ICS workforce development in energy or writ large. And then, the third piece, I'll talk about the market research. But, the third piece is to give all of you an opportunity to help us to inform our vision of what the strategic plan should be for CESER going forward, and we hope that that excites you to be able to play a role and to have a voice in what we need to do with the limited resources we have to be strategic in how we invest and what's going to make the biggest difference for the energy sector when it comes to the ICS cyber workforce.

So, we're looking for performers who have knowledge of two different areas. One is ICS/OT again, not information technology, but ICS/OT workforce training and development programs. And that first effort doesn't have to be focused on the energy sector. It can be any kind of ICS/OT workforce training and development program, because maybe somebody else is doing this really well, and we can lift that model and move it into the energy sector. So that first effort is not specific to energy sector, but as specific to ICS/OT cyber. The second effort is, what does the pipeline look like right now in the energy sector for people who are working with ICS/OT cyber professionals, so that second effort is probably the most tightly scoped. It's energy sector ICS/OT.

We've got about $160,000 available, and we're going to fund between one and two awards, depending on the proposals that are submitted. The projects are expected to be six months in length, but we do have the ability to give a one time, three month no cost extension.

So, let's just go a little bit into detail on the efforts again. The first one is the state of the ICS/OT cybersecurity workforce development and training. So, who's doing what out there in ICS/OT workforce development training. The second effort is the pipeline and workforce needs of the energy sector. And the third effort is helping us develop this workforce strategic plan.

Let's start with the first effort. Who's doing what? Like, who out there is actually being creative at doing ICS cyber workforce development? This might be competitions and cyber ranges, it could be apprenticeships that people are offering, it could be more formal academic degrees or certifications by a wide variety of performers, whether it's nonprofit sector, or even the vendor and original equipment manufacturers who also offer degrees and certifications. Maybe there are other workforce development methods, as I said, that are used outside of energy. Maybe they're used in manufacturing or AMO (advanced manufacturing) or other areas that we could lift and move into energy.

As part of the submission package, you'll notice that in the application there is a checklist

of different kinds of data. And this is really important. Please take a look at this checklist. We're going to be asking you of all the data that's out there. What are you going to specialize in? What are you going to be able to tell us? What can you bring to the table that's novel and insightful, so that we can build a data driven plan for what to invest in? This will be in the application and then in the narrative, in the longer form, you'll be able to expand a little bit about what is your what is your experience in working with that kind of data, and how you're going to use that data to address some of the concerns and issues that we raise in the application announcement.

The second effort is, as I said, focused on the energy sector and we're going to look at the ability of small medium and large organizations because the way people move through utilities that have less than 50 employees versus utilities that have more than 300 employees is very, very different. So, those pipelines of where an organization with 2,000 employees pulls its people is very different than the pipeline where an organization with less than 50 employees pulls its people.

These are questions about who's out there and how do they get their jobs. What are the skills? When an energy sector is trying to hire who are they hiring from? When somebody leaves the energy sector, where do they go? And how do the energy sector employers train their people right now to improve their ICS skills? How long does an ICS person stay with an employer? Is the average length of time 6 months, or is it 6 years? These are all pieces of information that can help us structure and design our investments in this workforce area.

Again, in the application, you'll see a checklist because we're interested in where do you want to focus? Is it that it's raw data on salaries, or is it analysis of on the job training? So, this checklist, please pay some attention to it and again, in the narrative, you'll be able to expand and describe how you work with these data categories and what you're promoting or promising in your proposal to be able to deliver. Now, in both efforts one and two, it's not listed here as dramatically, but we are also interested in whether you can find demographic data. So is there any information you can find that's robust enough for us to get a sense of things like, are there gender differences, or are there disability differences? Are there military differences in terms of military experience? Are there programs that just focus on a certain demographic category or economic development categories? So, we would like you to also look, if you can, at any kind of data you can collect that helps us understand the demographics of the populations that you're talking about.

Those are the first two efforts. The third effort is then giving you a voice and an opportunity to use your expertise to help inform us in developing this workforce strategic plan. We have a pot of funding available to invest in cyber workforce, and we would like to be as strategic and surgical as possible with that funding, so that we are investing in things that will actually make a difference for the energy sector. So, this is an opportunity to really work with us and partner with us, to inform where we go in the future, and we would love your help.

Eligibility, criteria are covered in the application. You must be a domestic entity. If you are a national lab or an FFFRDC, you can participate, but you can't be directly the prime, but you can be a subcontractor under an eligible entity. So, individuals are not eligible to apply, but if you know of other entities, again, you could probably come on as a subcontractor. If that's appropriate.

When we review your proposals, we're gonna be looking for 4 main categories. And the most important is technical expertise and approach and I'll break that down into how that 55% of the of the score is associated with very specific things. We're also interested, because sometimes we work a lot with sensitive data, what your own internal data security plan is. Budget and milestone is, of course, very important--how likely are you to complete the work within the 6 months in the budget that we've allocated? And then your project team composition obviously is important.

If you have somebody who has experience in ICS/OT, that will help a lot because you're going to find an enormous amount of information, technology workforce training and that's not what we're interested in. So having some expertise in ICS/OT, I would advise.

So, for the technical expertise, 55% of the points. 5% is what you're presenting. Is it reasonable? Does it make sense? 15% is going back to those application categories. Is the information you're going to be analyzing going to provide us with novel insights? So, we're really looking for the stuff that's hard to get right now and that's why we're asking for your help. We are looking for the ICS components of all of that data out there. 10% is on the appropriateness of the methods that you use for both data collection and analysis. And then 15%, which is the next highest category, is what are the final projects products that you're suggesting and how well do they align with what we've described in the opportunity announcement?

Again, this is just a brief overview of the announcement, and we hope that you will spend some time reading the announcement and the application so you get a better sense of exactly what we're looking for. We are obviously interested in your past performance and how closely your skill set of your team aligns with what we need to happen and the kinds of data we're collecting. Data security plan, as I mentioned, budget and milestones, work within budget, 6 month timeframe, $160,000 between the performers, and your project team composition.

That's a quick summary of what we're looking for. We really are excited to finally put this out because we know that there is information out there that will be useful to CESER to help us build and design investments that can actually move the needle and help our industry, accelerate the buildup of skills both within their incumbent workforce and accelerate the pool of applicants who are qualified to do ICS cybersecurity, and that they're available for the our industry to hire. So, with that I'd like to pass it back to Meg. Thank you very much.

Meghan Camello, TechWerx:

Awesome. Thank you, Cynthia, if you go to the next slide. So, this opportunity, as Cynthia mentioned, is very interesting. The deadline for this opportunity is the 23rd of December at 5p.m. Eastern Standard Time, although we always recommend submitting it early case any technical issues arise.

As I mentioned earlier. You'll see on this slide, December 11th at 2p.m. Eastern Standard Time, we'll be hosting office hours, where we'll be answering your questions about this opportunity.

In the meantime, if you have any questions that can't wait until the 11th, feel free to email us, or contact us on our website through the contact us form. Our email is info@techwerx.org. The website is the best place to stay up to date, not only on this opportunity and any updates that might happen, but also for future opportunities. We appreciate you taking the time to listen and watch this webinar today, and we're excited to have your applications. Thank you.