TechWerx State of Industrial Control System Cybersecurity Training Opportunity Office Hours Transcripts
12/11/2024

Shane Hamstra, TWX:

Well, good afternoon, good morning, everyone depending on where you're joining from today. Thank you so much for being here for these office hours. Just a few quick logistical announcements before we begin today. If you need to submit any questions or comments or concerns with any troubleshooting for Zoom, please use the Q&A portal. The Q&A portal is open throughout the session and you can submit questions there, comments, and of course, if you need technical assistance, please let me know in that Q&A portal. Today's session is being recorded and will be offered as archive and you'll be notified by email when that's available.

Finally, if you would like, you can use the captioning and transcript options provided by Zoom, by clicking on your CC option on your Zoom toolbar and clicking on show subtitles. That's just for your own individual screen, if you'd like to utilize those. Well, thank you so much again. And now I'll hand things over to our moderator to kick us off.

Adam Klich, TWX:

Alright. Thank you, Shane. Hello, everyone. We're very excited to host this office hours for the State of Industrial Control System Cybersecurity Training opportunity. This opportunity is being funded by the Office of Cybersecurity, Energy Security, and Emergency Response, or CESER, at the Department of Energy. So next slide, please.

If you're not familiar with TechWerx, we're a new innovation hub managed by RTI International in support of the Department of Energy. The goal for our hub is really to facilitate connections among the federal government, academia, nonprofits, and small businesses across the US. To hear about any new opportunities that come up through our hub or updates on this specific opportunity, we recommend you follow our page on LinkedIn, as well as sign up for a newsletter via our website on techwerx.org. Next slide, please.

A couple of housekeeping items before we get started again. Please use the Q&A chat for all the questions that you have. On the Q&A function of zoom, you're able to vote on the questions that that are posted there. So please look through the questions submitted, and vote on the ones that you want to make sure that they'll be answered. We should be able to get through quite a few questions today, but if we do end up running out of time and not covering all the questions submitted, we're going to still collect all of them and work offline to have them answered. All of the questions that are covered during the webinar, and after the webinar, will be captured and posted on the FAQ section of the opportunity page on our website.

Also, we do not allow any AI bots, so, Otter AI or any of those for the meeting per DOE requirements. You shouldn't need them, because this session is being recorded and the recording as well as the transcript and the slides will be available on our website within a couple of days. Next slide, please.

Okay, so I'm Adam Klich, I lead the TechWerx hub here at RTI, and today I'm joined by the CESER team. I'm going to pass it over to them to do a quick recap of the opportunity, and then we'll get into the Q&A portion of the session.

Cynthia Hsu, DOE CESER

Great thanks. Great to be here. I'm Cynthia Hsu. I'm one of the cybersecurity program managers in the Department of Energy's Office of Cybersecurity, Energy Security and Emergency response. I have a number of hats that I wear. But let me just introduce the rest of the team, and then I'll go into some details about the proposal. Fania, would you like to introduce yourself?

Fania Barwick, DOE CESER

Hi, good afternoon. I'm Fania Barwick. I'm the implementation manager for the RMUC program, and I am also the implementation manager for the workforce program that Cynthia is the program manager for. Steve.

Steve Lindaas, DOE CESER

Hi. My name is Steve Lindaas, and I am a science technology policy fellow. I'm working to support all aspects of the RMUC programs, this one as well as others.

Cynthia Hsu, DOE CESER

Thanks, and our other member is Kate McGrath, who is out of the office for another few weeks, and we will be great grateful when she comes back to us. So, if you could go to the next slide.

We're here to talk about an opportunity that CESER has put together. So many of you probably know me associated with the RMUC program, the Rural and Municipal Utility Cybersecurity program, which is focused on small and medium utilities and public power and cooperative utilities. This is a different hat. So, if you know me under that guise, this is something different. So, this is under our workforce development funding, and this is meant to look at workforce across all of the energy sector. So, this is all the investor owned utilities, all of oil and natural gas, and hopefully depending on the responders here in this audience and in this community, it might even touch on renewable energy and distributed energy technologies. So, this effort is very much across the energy sector. If you know me with another hat, I just reorient to this.

CESER is the office, It's the ESF, the Emergency Support Function 12 Office in the nation for any emergency having to do with energy security. We have a couple of other functions in addition to that emergency response function. We do a lot in risk assessment and risk mitigation, there's a whole section on R&D and technology development. We do a lot of sector collaboration with SLTT and the energy sector, representative agencies between intergovernment, and with the private sector. And we do a lot of research on energy supply and some of the critical risks, again, through the risk assessment risk mitigation functions. Today, we're here to talk about another area of CESER's portfolio, which is what will CESER do in the future for workforce development for ICS and operational technology, industrial control systems and operational technology (ICS/OT), cybersecurity, as we know for those of you who are in the field finding ICS/ OT, cybersecurity, finding people is even more difficult than finding information, technology, cybersecurity people, because the information technology, cybersecurity space is pretty broad. And there are a lot of players in that space.

CESER's real unique piece is the industrial control systems operational technology part of cybersecurity. So, this opportunity that we're going to be talking about today is really focused on that niche ICS/OT cybersecurity. The work that we have put out and we are asking for partners to help us do is going to feed into what myself and this team are responsible for, which is developing CESER's strategy for what investments they will make in cybersecurity workforce in the future. So, this is all feeding into that strategy development. So next slide.

So, there are a couple of specific things we're looking for. But the overall details: we're looking for entities that have knowledge of ICS/OT workforce, because there are some very unique things in the ICS/OT workforce world in terms of responsibilities and hiring practices and pipeline that are different than the general, IT security. So, we're really looking for people who have the ability to go out and find information specifically about the ICS/OT workforce, and we're looking for people, again, I start with the unicorn and we'll see what comes in, but let's go for the whole unicorn. Ideally, ICS/OT workforce in the energy sector. There are a lot of other people in ICS/OT in other sectors, but we're really focused on energy. So, if you have a background in the energy sector ICS/OT cybersecurity, and you're interested in partnering with us. That would be awesome.

We can mix and match a little bit. Here we have $160,000 available for up to one to 2 awards, and we expect the projects to be 6 months in length with the ability to extend if we need to, with a 3 month no cost extension. Next slide.

TechWerx State of Industrial Control System Cybersecurity Training Opportunity Office Hours Transcripts
12/11/2024

So, a little bit about what we're doing. And if you've already read the proposal, you probably know this, there's three different efforts, and you can propose in one, two, or all three efforts. The first one is the state of what's happening out there. So, this is looking at and giving us knowledge about who's already doing training for upskilling existing workforce and also training for bringing new people into the workforce we're looking at, not just academic training. But we're interested in what's also on the cutting edge, whether it's ranges or cyber security clinics or apprenticeships and other kinds of on-the-job training. We're looking at training providers like original equipment manufacturers. A lot of the OEMs give training that's out of the federal government outside of DOE, if you're aware of that not-for-profit sector training. So we're trying to get what currently is available, because what we would like to do is either supplement or leverage what's available instead of funding things to duplicate something the private sector and nonprofit sector are already doing. Having that background and that situational awareness of what everybody else is already doing is going to be very critical for us to make those strategic investments.

We're also looking for the pipeline, and by the pipeline, in the end of this something that I think would be innovative for us to understand is, where do the ICS cybersecurity employees currently employed come from, and where do they go when they leave.

So where do they come from? Is it that people out of an academic training background are getting hired into the energy sector as an ICS/OT cybersecurity employee? Or are they coming from consulting groups? Or are they coming from some other place? Because that pipeline helps us understand where we need to invest to create new employees. And then where are they going? Are they moving up the ladder? Do they start? Maybe in a municipal utility, and then they get hired by a larger utility. And then they go to the consulting world. So understanding that process of how they're moving along as they develop skills is probably the key goal of this effort. Number two, and anything that you can do to help illuminate that process will be helpful to us in making strategic investment decisions.

And then the third one is all of this is background data, but we are also inviting you to come to the table with us and give us your suggestions on what we should be doing. How do we create this workforce strategic plan given this very, very tight market, and that a lot of people with this skill set really are in limited supply? A friend of mine said it's sort of like a flight with two legs; in the first leg, you develop a certain amount of skills either in engineering or in cybersecurity, and on the second leg of the flight you combine those, and you really get into the world of control systems in cyber security.

This so that you know what we're going to be looking for-- shouldn't be a surprise that the technical expertise and approach is the highest thing we're looking for. It's detailed on the website and the opportunity announcement that TechWerx hosts. We're also looking for project team composition, so, it's going to be important to us that you demonstrate awareness of ICS/OT cybersecurity. So, if your team right now is only IT cyber-focused and you would like to participate in this, it's going to be very important that you bring in some expertise that can help you understand what's unique about ICS cybersecurity and guide the work that you're doing with that knowledge.

I think that is the last slide, so I think I pass it back to Adam and we wanted to leave a lot of time for you if you have questions. That is the purpose of this. So, Adam.

Adam Klich, TWX

As a reminder, the informational webinar or objective strategic session is pre-recorded and it's posted on the opportunity page of our website. So, if you have not watched that we recommend watching. It's where Cynthia goes a little bit into more details about the opportunity. We're hosting the office hours today, and the deadline for the application is on Monday, December 23rd by 5PM.

We recommend submitting your application prior to the 23rd so that if you do have any technical issues, we can work through it, and you won't miss the deadline. We expect the review and selection to go over like one or two months, and then, you know, once the selections are made by DOE, we'll get into negotiations, get the agreements in place, and then the announcement for the selectees and activities are expected to begin around March. And again last for about 6 months with a potential option for a no cost extension there for 3 months.

With that we're going to get into the Q&A portion of this session. There's a Q&A button in the bottom of the screen, feel free to go in there and type in your questions, or vote for questions that have already been submitted. So, we already have a couple there. And we're going to get started on those.

First question, Cynthia, are you looking to extend programs already in existence, such as the NIST funded US Cyber Games with capture the flag challenges specific to critical infrastructure?

Cynthia Hsu, DOE CESER

So, we're not actually funding programs in this effort, we're funding market research. What we would like to do is understand what other programs there are out there like the US Cyber Games. So, this is a market research proposal, not funding to start a program or expand an existing program. Does that answer your question?

Adam Klich, TWX:

I think it does. Yes, thank you.

Second question: for the gap analysis, is there an expected pool of people that will be provided for input on the gap analysis? And is there a minimum number of people contacted, expected, or as part of the program developing those contacts?

Cynthia Hsu, DOE CESER

A couple of different layers there, and I'm sorry I'm looking to the side because I can't see the question itself and it's a long question. So, I'm going to look to the side. Is there an expected pool of people that will be provided for input on the gap analysis? No, that's going to be up to the performer. So, we're looking for the performers to have input and to provide us with input on who those people should be and where the gaps are. Not sure if I completely answered that is there a minimum number of people contacted expected. That will be something that you propose back to us, and if you make it into negotiations, we'll have that conversation with you. So, the market research is not necessarily for you to tell us who all is doing this, although we want to know who all is doing this, but it's for us to have situational awareness about what is happening.

Adam Klich, TWX:

Question on topic one. It is stated that no contact should be made to providers, relying only on publicly available information. For topic two, will it be expected or appropriate to contact employers and other professionals directly? Or must that also be public info only?

Cynthia Hsu, DOE CESER

So, we're assuming that most of this can be done with open-source intelligence with without having to do surveys or phone people, and that was primarily to keep the cost down. If you think you can accomplish this in a thorough manner, with the price point of the funding that's available by doing individual reach outs, I think we would be open to that. But I don't think you're going to be able to get a comprehensive view of all of the opportunities with this funding, if you're doing one on one conversations. So, the first one, we think, can be done with open-source intelligence, the second one, it's possible to do it with open-source intelligence if you understand some of them and you have access to some of the commercial job market information already out there, and the public job market information already out there.

Feel free to ask follow up questions if I'm not getting at what you're asking for in this.

Adam Klich, TWX:

Okay, next question. With the lack of standardized job titles for ICS/OT cyber security responsibilities, what unexpected roles are you all finding data under like engineer since that was mentioned as a major research challenge on the initial webinar?

Cynthia Hsu, DOE CESER:

So, I wish I could answer that. I think that is part of the challenge of finding out where all these go and what are the appropriate search terms when you're looking at job roles. Because in the world that I work in primarily, which is smaller utilities, the person who's responsible for cybersecurity might also be the person responsible for grounds maintenance right? So, in larger utilities, sometimes that cybersecurity, responsibility is hidden under various technical roles that are in operations and engineering, and sometimes it falls under the more common and well-defined roles that NIST has helped us with in terms of job roles, but there isn't the equivalent commonality like there is for it for the ICS/OT cyberworld. And so, there aren't really easy search terms. And that is why I think it's really important that people who are familiar with ICS cybersecurity be part of the team so that they can help you work through what are some of the search terms to use.

Adam Klich, TWX:

Follow-on question to that one. Will we have access to the research you've already done?

Cynthia Hsu, DOE CESER:

That one's pretty easy because we have not. There are some things that we've learned from open-source information already. So, the White House report on cyber security. But almost everything that's already been published, there's not additional information we're going to be able to provide you.

Adam Klich, TWX:

Question. If the preference is to leverage or supplement existing programs, what's the goal or restrictions on that post research funding, staff advertising or recruiting efforts, equipment for hands on training.

Cynthia Hsu, DOE CESER:

I'm not sure I understand the preference. We're not necessarily leveraging or supplementing existing programs in this effort. What we want to understand is what are the existing programs already doing and what's the gap that's not being filled by the existing programs. So, what we might do in the future, based on that strategy document, could be a combination of the two. It could be that we're investing in things that don't already exist, or it could be that we're investing in something that is done over here in manufacturing, but might be applicable to the energy sector, or is taking something that's happening in the energy sector, and it could be ramped up or fill in the blank. So really, the goal here is to get a state of the state and the understanding of what's already happening and what the gaps are, so that we can focus our investments.

Adam Klich, TWX:

Next question. Would we be able to use prior research or group has already conducted on this topic, and additionally, are you interested exclusively on ICS/OT roles in the energy sector, or broader to a variety of sectors?

Cynthia Hsu, DOE CESER:

We would certainly be open to using prior research, if there is research that you can leverage to share with us. Just understand that the information that you bring to us is coming to the government. So just make sure you're allowed to share that information with us, but we are certainly open to you leveraging existing research or prior research that you've done. For the second part, are you interested exclusively on ICS roles in energy sector. Look at the two efforts. So, one of them is very specific to energy sector, which is topic two, effort one is broader, so, if there are ICS/OT cyber security, let's say there's an apprenticeship program for ICS/OT cybersecurity in manufacturing. We'd still want to know about that. So effort one is much broader, we're looking specifically for ICS/OT, but the sector isn't defined in effort two, it is very specific to the energy sector, because the pipeline that we're interested in is the energy sector pipeline.

Adam Klich, TWX:

Question. Should the proposal address all efforts, or could it be focused on an effort?

Cynthia Hsu, DOE CESER

So, this is your choice. You can do one. You can do two, or you can do all three. So yes, you can just focus on one effort and within the effort. So, for example, under effort one, there's a whole list of entities that might provide training. And ideally, we're looking for things that are going to shed light on areas that aren't already available. So right now, I'm not aware of anybody who's consolidated across the energy sector or any of the critical infrastructure sectors what kind of training the OEMs do.

I'm not sure there's a really good compendium of the kinds of trainings that the nonprofits do in ICS. And there's a lot of training that some of the nonprofits are doing in ICS. So academic is probably easiest for us to get and might be of a lower interest in terms of having to choose across priorities than somebody who's proposing to do something where the information doesn't currently exist at all and will actually really shed some light in a new and novel way on what the challenges are in the ICS cyber workforce.

Adam Klich, TWX:

Next question, what are the guidelines or limitations on subcontracting or partnering?

Cynthia Hsu, DOE CESER:

Adam, do you know what that one is? I don't know what the answer is.

Adam Klich, TWX:

No, there are no limitations on subcontractor partnering beyond the, you know, we have requirements on organization being US-based and those things, so they also apply to subcontractors, but, otherwise you are able to have a partner on this on your proposal.

Next question. Regarding is strategy, what is the team's current perspective on where the talent pipeline begins?

Cynthia Hsu, DOE CESER:

I love that question and I could probably spend 30 min opining on it. So, I think it depends on what kind of energy sector participant you're talking about. So, for oil and natural gas, I have a lot less visibility into what a production facility would need for a pipeline versus what a distribution facility would need for a pipeline. I have much more of a background in the electric sector, and primarily with the smaller and medium sized entities, and there the pipeline might start with somebody who volunteered and then became a lineman or started doing staking, and then showed some aptitude for technology and became a technology person for the utility, and then suddenly found themselves because of the technology person responsible for cyber security right? And it was just all an internal flow for a large IOU, maybe the pipeline is, like I said, they're hiring from a smaller utility where the utility itself doesn't have anybody labeled as a cybersecurity ICS staff role, but it turns out that the work that they're doing includes ICS cybersecurity skills. And then they move into an ICS cybersecurity staff role at a larger utility.

These are all black boxes to me, and all I have are anecdotal stories that people have told me, and part of the purpose of this effort is to take it out of anecdotal and try and wrap some numbers around it, so that we have a better sense of what that pipeline looks like.

Adam Klich, TWX:

What other questions do you all have about the opportunity?

There is one Infragard/ FBI is working on a state of AI in critical infrastructure research project and leading one of the research projects. Our research includes cybersecurity applicable to AI in the energy sector. Would you like to receive this research?

Cynthia Hsu, DOE CESER:

Totally happy to receive research related to this. I think you can just forward it to Adam, right? Can't you just forward it to TechWerx? Unrelated to this, and it will come to the team.

Adam Klich, TWX:

Yep. Feel free to send it to us at info@techwerx.org, and we'll forward it to the CESER team.

Cynthia Hsu, DOE CESER:

And feel free, if any of you want to share your own insights in this forum, because I'd be interested in in what you're doing as well, but if you have other questions, this is the primary opportunity to sort of sort of poke at the proposal, and see what's in there that might not be so obvious in the writing.

Adam Klich, TWX:

We'll hang around for a few minutes to allow people time to type them in.

Cynthia Hsu, DOE CESER:

So, I'm hoping that some of you are interested in this because this is an area that's really in desperate need of focus. There is a lot of work on workforce and IT cyber. And we are in need of people who understand the nuance of what's different about the workforce when it comes to ICS, and anything that you can bring to the table to help us understand how to better use the funding that we have would be appreciated.

Adam Klich, TWX:

So, here's one more question. One of the main things we found in our workforce development research is that ICS/OT jobs are quite rare nationwide, especially compared to IT roles. Are you looking for a specific threshold for sample size?

Cynthia Hsu, DOE CESER:

I think I would be looking for proposals of what you think is an appropriate sample size, and that's something that we can negotiate. There are, you know, across all of the energy sector, there are actually quite a few people doing this, but it's not called this. And then within some of the high-end firms that do ICS cybersecurity that can pay a higher price point, there's obviously another whole swath of people. But in general, this community is incredibly small, so that observation is true, and it's extremely small relative to IT cyber people, and, as we all know, there is a dearth of IT cybersecurity people in general, in terms of finding the people that you're willing to come into your organization and have the skills and experience that you need. We could talk about what entry level means.

Adam Klich, TWX:

We'll being around for a couple more minutes. And then, if there are no other questions, then we may close out. But here's another question. We'll stay around as long as you have questions, so keep them coming.

To clarify the earlier question regarding how the strategic plan ideally would leverage or supplement existing programs versus create new, I know this research will help inform that, but to help focus our research, do you have any ideas on how the funding would be used to support existing programs (hiring additional staff to teach, supporting hands-on training events, advertising, or recruiting efforts, etc.)?

Cynthia Hsu, DOE CESER:

So, I may not. And, Daphne, if I don't fully answer this question, do shoot a new one in. So, this $160,000 is just market research. Maybe you're talking about funding that might be available in the future.

Adam Klich, TWX:

She said right.

Cynthia Hsu, DOE CESER:

Okay, so you'll probably have heard this answer before, and you might hate it, and I would understand why. But we can't talk about what we might do in the future, but our goal is to leverage this work so that what we do is informed. And I realized that's not the answer you wanted.

Adam Klich, TWX:

Question here. Speaking of security, our work security won't allow us to access TechWerx or any of the other -werx websites. Is there an alternative DOE website where we can access FOAs?

Cynthia Hsu, DOE CESER:

So let me take one nuance of that. So, what this opportunity is, is it’s not really a FOA, a funding opportunity announcement which is released by DOE directly through one of our one of our partners. This is something different than a FOA and Adam, maybe you can clarify what this is relative to a FOA.

Adam Klich, TWX:

Yes. So this uses a different contract vehicle that DOE has with RTI in this case for TechWerx, which is a partnership intermediary vehicle. The contracts that will come out of it will be a, B2B contract between TechWerx and the performer, and it will be a fixed price milestone-based contract. So, it's a little bit different than a regular FOA that comes directly from DOE in terms of the application process. Really, it's through the website on the application portal. The application system on the website has some information that we collect as part of it, so, we don't have an offline version of the application. Most of the application is captured on a Word document and the templates provided on the opportunity page, but the submission system is through our techwerx.org website because there are some other check boxes and information that we collect as part of the system. So, there is no alternative to do it offline. It has to be done through our website, and if you are having security issues, and there's anything that we can do on our side, please do reach out directly via email and we can try to work through it.

As a reminder, if you do have questions that come up between now and the deadline for the for the application, you can either use the contact form directly on our website or send us an email at info@techwerx.org, the email in the chat. We'll be happy to try to get you an answer or support if you're having any technical issues.

Cynthia Hsu, DOE CESER:

Last call anyone else.

Adam Klich, TWX:

Well, thank you all for joining. We do ask that you take a very brief post office hour survey to help us make sure that future office hours and webinars we can improve on the process and bring the right information to you. So, the link is in the chat, and again, if you have any questions between now and the deadline, feel free to send us an email and we hope to see your applications come in soon. Thank you, everyone, for joining.

Cynthia Hsu, DOE CESER:

Thank you all.