# Q&A: Cyber Security Issues and Requirements – Jeff Dagle

Q: On the theory that there's not a lock that can't be picked and a safe that can't be cracked, I think cyber security is a bit of an oxymoron, right? We all share the same goal and the same concern. But I think the vast majority of people in this room are not cyber security experts, and we're pretty much dependent upon the vendors and the experts who are in the field. I guess my concern and my question is this: I think we need to set up some defined due diligence around cyber security instead of creating some kind of expectation that we're all going to guarantee that something will never ever happen. Because we cannot guarantee that. Nobody knows what the vulnerabilities are until somebody has tricked the system and found the vulnerability. And at first I didn't think that something as simple as meters would be vulnerable until somebody outlined a very nightmarish scenario to me about how a virus spread through meters could actually shut down a large number of generators. So it's kind of an open-ended question, but it's a concern that I have about cyber security. I mean, we have pretty sharp people in our IT infrastructure and architecture groups. They share this concern. But there's only so much we're going to be able to do.

A: Great. It's a good comment, and I agree with that. And the challenge is: What are the best practices that we can deploy to minimize the risk that we're taking? But certainly, part of that equation that you point out is that we need to be realistic in our expectations, and I certainly agree with that. 100 percent security is almost like saying we'll never have another blackout. There are certain things you just can't guarantee. And so that's a good comment. Now the path forward: I really think that when you work with your DOE project manager, and you see the comments on your proposal, hopefully it will make more sense, that this is sort of the feedback that you're getting on your project. It's very hard for me to make statements that apply to all 100 of you in an overview.

Q: Leading up to this, there was a lot of discussion with the NIST standards in draft form. When I looked at the contract, when I've looked at the presentation, there's no mention other than "applicable standards." And so what can we expect as those become final from DOE as far as applicability, what you're expecting from us as far as implementing those to what makes sense and so on and so forth.

A: Right. Great point. And the challenge, of course, is that NIST is on a very aggressive, fast-track timetable to develop a roadmap of applicable standards. Neither DOE nor NIST are standards-development organizations. And so there's a requirement—a need—to work with standards-development organizations to develop those standards that are appropriate. And yet we have this project that we're launching with the $3.4 billion, realizing that standards are probably going to be developed at some point in the future that are going to apply to these projects. So the way that we handle that in the FOA was to say, we want you to tell us what standards you're going to follow today, what industry practices you're going to follow today, and then what strategies you can put in your project to apply to future standards that might get developed. It's a little fuzzy for us to look in our crystal ball and estimate where those standards are going to be one, two, three years from now. We just don't know.

Q: Right. But let’s say that they do become ratified. Can we expect feedback from our project manager saying, okay, these have been ratified; now we’ll work with you to fully review it, and here’s what we want you to look at.

A: This is not any sort of official standpoint or statement. This is just sort of my assumption. My assumption is that, whether or not you feel compelled to follow those standards is sort of separate from this grant process. You’re going to have other regulatory drivers that are going to put pressure on you to follow appropriate industry standards. And I don’t think that pressure’s going to come from this grant process.

Q: Can we expect anything to come up in the grant award contract regarding cyber security, or is it just there that we need to deal with it?

A: Well, there will be specific feedback as relates to cyber security as it relates to your project that will be part of the grant and the award process. The comment about it not applying was the standards and what eventually gets written.

Q: I have a few related questions that might be a little more specific than the last gentleman. We are—and I think there are others of us here today—a power grid operator, and as such, we are NERC-registered, reliability coordinator, balancing authority, transmission operator, transmission planner, and a couple of other things.

Q: You missed generator operator.

Q: Thank you. And as such, we have in place a series of procedures already for compliance with the NERC CIP (critical infrastructure protection standards) for physical access and cyber access to our systems. First of all, let me ask: In the existing law, in the 10 CFR, are there additional standards in there that we need to be aware of? And I guess related to that would be, do you anticipate adopting hard rules or additional requirements beyond what’s in the NERC CIP?

A: The short answer to that is yes. And that’s because a lot of this smart grid technology that we’re talking about here is sort of outside the scope of the NERC CIP requirements. Particularly if you’re not a bulk power system as critical assets, it’s a little tricky there. Because those things don’t necessarily apply to the NERC CIPs. Yet there is a reliability concern associated with wide-scale implementation of those. And if it wasn’t for the investment grant process, DOE would have no requirements to the industry to levy that. That’s really FERC’s jurisdiction and domain. And there’s various things going on there about where FERC’s jurisdiction ends. But what’s different here is that you’re getting federal money to go into this project, and so that’s where the DOE has the authority to put the cyber security requirements on the project. It won’t extend beyond the bounds of the project.

Q: Just a couple clarifying questions. Are there existing requirements out there now? Or are you developing them yourselves? You know, critical infrastructure protection?

A: No, that’s under the purview of NERC.

Q: The cyber security requirements for smart grid technologies, you will be developing additional requirements for those technologies?

A: The comment was alluded to earlier with the NIST roadmap, and there are some cyber security concerns associated with that. And so that would be the place where those are being developed.

Q: But they’re being developed. They’re not available yet.

A: Correct.

Q: Okay. Thanks very much.

Q: My questions are very similar to his. American Transmission Company is only a transmission operator. We are a NERC-registered transmission owner, transmission operator, transmission planner, and planning authority. The only technology that we’re installing will be installed on the bulk electric system on 100 KV and above. We will then be required to certify every quarter to our two regional entities that we are compliant with the cyber security requirements and the data concentrators. Our project is a fiber optic project and a phasor measurement unit project. Our data concentrators are going to be located inside our EMS system operations center, which is both cyber secure and physically secure. And I’m trying to apprehend where it is that the jurisdiction of the DOE resides with respect to additional cyber security on facilities that are exclusively the jurisdiction of the FERC and NERC. Once the phasor measurement unit gets bolted onto our utilities, it becomes an integral part of the bulk electric system, and I can’t differentiate it one from the other. Because I can’t certify to them that I’m compliant if I’m telling you that it’s not part of the bulk electric system. So I’m having a bit of difficulty concerning where the pathway lies that we’re going to have to have any additional requirements over and above what we’re already required to comply with.

A: Right. And I don’t have your stuff in front of me, so I can’t tell you that there aren’t any additional requirements. But when you sit down with your DOE project manager and you get your briefing on your cyber security requirements, it may be that you’re already fully covered because of the NERC CIP requirements that you’re already following.

Q: My manager of security will be very happy to hear that.

A: And I put a lot of caveats on that. You ask specifically what the jurisdiction is in DOE. Well, it’s not that we have a regulatory requirement to compel you to do that. It’s part of the funding of the project. So if in the view of the DOE project manager, there’s a cyber security concern that isn’t addressed in your project plan, they can ask for that to be changed in the project plan to the satisfaction of DOE as a condition of getting the funding.

Q: And I think you can tell from my questions that my approach to my cyber security plan is going to be, I'm compliant with all of the NERC requirements, and I'm going to do my quarterly reporting to all my regional entities. In the event that I declare a self-report that I'm in violation of my cyber security standards, I will then report to the contract officer. So my inclination is that the two of them are going to be virtually co-extensive.

A: And that may be a really good answer—and again, in your situation as a transmission operator, I think you're on pretty solid ground. You'll find out when you talk to your DOE project manager. But consider another organization that is putting in a project that is associated with distribution stuff, and they say they're going to follow the NERC CIP standards. Well, it doesn't take a rocket scientist to figure out that they don't have any critical assets that apply to the bulk power system. So per CIP 002, they don't have to do anything. And so if they tell DOE, I'll just follow the CIP standards, that means literally they don't have to do anything because they don't have any critical assets that apply to the bulk power system per the definition of CIP 002. And CIP 339 only applies if CIP 002 applies, right? So if they put that in their proposal, and we say, sure, that's fine, literally that means they don't have to do anything. So that was my comment about compliance does not equal security. You can be fully compliant with the NERC CIPs and not have to do any security. And with this program, we think we can do better than that. So again, I'm not trying to pick on your project with that comment—you may be in great shape. I'm not trying to pick on the NERC CIPs either because they have played a very important role in helping to enhance security of the nation's infrastructure. But again, you have to recognize that the NERC CIPs are really only intended to protect the bulk power system, and they're really geared around critical assets. And in the process you define your critical assets and your critical cyber assets; then all of the security stuff applies to those. And if you're putting in AMI or doing another distribution automation project, it's not clear that the CIPs really do apply there.

Q: One follow-up question: PMUs are not critical assets and would not ordinarily be deemed critical assets. Did I infer—incorrectly, I hope—from your last comment that anything that's installed will be deemed critical for the purposes of cyber security?

A: It depends on the application in which it's intended to be used. So if somebody tells me that they want to put in a PMU that's going to feed some sort of control system, then it could create a reliability issue on the grid. We would like to see cyber security measures applied to that project commensurate with the risk that's being introduced. Whether or not that's considered a critical cyber asset per the definition of CIP 002, we're less interested in that. We're more interested in making sure that we don't introduce a cyber security vulnerability that would put the nation's electric infrastructure at undue risk.

Q: I would only request or at least ask you to give consideration to not using the term "critical" if in fact you think it's necessary to be secure. When you attribute the term "critical," that raises a huge level of compliance requirements that are triggered by the

CIP standards. If in your mind it's something that warrants cyber security, those of us who are concerned about the criticality of critical assets… I would only ask that you refrain from calling them critical.

A: Okay. That's a very good point. I invoke that term in our Q&A here, but you raise a very important point, and this is worth making clear. If we come to a conclusion that we need to do cyber security as a result of this project, as a result of your receiving federal dollars and putting in some sort of smart grid project, and we want you to jump through some cyber security hoops, that does not, in our mind, trigger NERC compliance stuff. Your NERC compliance activities that you have to do to be compliant with the NERC CIP standards—that's a separate issue. So if it's not a critical cyber asset by the definition of 002, then you would tell your NERC auditors, here's our assessment of the 002 report, and 003 through 009 don't apply. But you could be doing 003 through 009 to satisfy the DOE side. It doesn't trigger all the paperwork you need to satisfy the NERC auditors, right?

Q: That conversation with the NERC auditor will go a lot better as long as you don't call it critical. If you don't call it critical, I don't have to try and explain it to him.

A: No, I understand. So our approach here isn't to go into your organization and decree that there's critical cyber assets. Our approach is to look at it from a project-specific standpoint: What are the cyber security requirements that are required for your project?

Q: Very good. Thank you very much for that clarification.

A: Some of us are already having to do CIP on our transmission grid. Would you be willing to stand there and say that we would not have to do anything more than what is required in those CIP standards on the distribution system, and maybe even less than that?

A: No, I don't think that's what I said at all.

Q: No. Would you be willing to, though?

A: No, I don't think I'd be willing to say that either. Again, I didn't want to talk about each of the projects, one at a time. That's not really why we're all here today. So your project manager will convey to you, based on your project, what they see as the issues that DOE feels you should be addressing. If you don't feel those are reasonable, it's called negotiation for a reason.

Q: But it is fair to say you wouldn't go past what is required in the CIP standards today.

A: I'm just not sure I'd make that statement that authoritatively.Again, the main thing that's hanging me up on the CIP standards is really CIP 002. In my personal opinion, 003 through 009 are pretty good. And so if you're doing everything that's 003 through 009 on your project, I think you're in pretty good shape and you have a good leg to stand on.

Q: Right. If I would set CIP 002 aside and apply the rest—if I went to that level on distribution and whatever else we're doing smart grid—that would be reasonably satisfactory.

A: In my personal opinion, I think you'd have a really good leg to stand on.

Q: Generally, when might we expect to better understand what the recommendations would be in terms of what might apply? One of the reasons I ask is, I have the honor of standing before our commission tomorrow to talk about this and litigated proceedings, so I was kind of curious: What can I tell them? I get the impression it's going to be a case-by-case basis, so you can't give me a general feeling.

A: Yeah, I really have no idea what the plans are among the six DOE project managers, how quickly they'll be ready to roll out. I highly suspect you won't get any information by tomorrow. You can pretty much put that one in the bank. But again, I haven't talked to the six project managers, so I just have no feel for what their schedule is. And as you might imagine from listening to today's discussion, we're getting a lot of feedback from you all, and that's helping us better understand what to ask for in this negotiation. And there's obviously more than the cyber security. There's a lot of other things that they want to bring up with you on your project. And so it's just sort of getting all that information together before they can engage with you.

A: And I'm not sure the six DOE people even know what the feedback is yet. So if you ask them for their feedback in this informal meeting this afternoon, I don't think they have that information yet. So I just don't want to set any expectations here that they have this information and they're waiting to give it to you. It's still being gathered.