Presenter Responses to Attendee Questions –
EnergySec/Deloitte Webinar May 20, 2015

NOTE: The following are responses by the webinar presenters to questions submitted online during the webinar on Issues with CIP-002-5.1. None of the responses below should be interpreted as compliance guidance. Only your Regional Entity can provide authoritative compliance guidance; we recommend you discuss all questions with them.

Question 1: We have heard that 'adverse impact' may also be extended to consider the lack of full capacity (e.g. not having the full capacity of a generating plant). That seems to be an expansion of potential scope if the generating unit is still providing power but at a reduced level.

Response: The definition of BES Cyber Asset refers to impact on the BES, not to the *level* of that impact. This seems to mean that, even if the loss or misuse of a Cyber Asset would only result in a small adverse impact on the BES, the Cyber Asset is nevertheless a BES Cyber Asset.

Question 2: Can you provide a Transmission SCADA system example? (This was in reference to Tom's slide 13, where he provided two examples of his method of determining whether there was "adverse impact" as required in the BES Cyber Asset definition)

Response: It is hard to believe that a Transmission SCADA system could ever *not* have an adverse impact on the BES, if lost or misused. Using the two questions discussed in the presentation:

1. *Does the Cyber Asset impact the asset or Facility it's associated with?* The asset in question is probably a Control Center. If the Transmission SCADA system is lost or misused, it will almost definitely impact the Control Center it is part of.
2. *Does this necessarily translate into an impact of the asset or Facility on the BES itself?* Again, it would be very hard to argue that there isn't a BES impact if the Control Center is not able to perform its normal functions because the Transmission SCADA system has been lost.

Given that both questions have been answered "yes", and that the impact on the BES is very likely to be within 15 minutes, the Transmission SCADA system is most probably a BES Cyber Asset.

Question 3: How about VOIP? (This is also in reference to Tom's slide 13, where one of his examples was a "Phone System". Tom demonstrated that his methodology for determining whether there is "adverse impact" leads to phone systems not being BES Cyber Assets)

Response: Even if the phone system is a VOIP one, the same analysis applies. While the answer to the first question (under Question 2 above) is "yes", the answer to the second question is "no". This is because, were the phone system – VOIP or not – to go down and should an urgent action need to be taken like dispatching a peaker plant, there would still be other alternatives which would eliminate a BES impact in 15 minutes. For example, the controller could use his personal cell phone.

Question 4: Is there any indication that the Regions are adopting the use of BROS (BES Reliability Operating Services) in their audit approach?

Response: It's likely they will, but the bigger question is in what way they will use them. As with everything else, check with your RE about this. Also note that the recent NERC Memorandum on communication devices stated that the BROS are not the sole criterion for identifying BES Cyber Assets. Entities should not exclude Cyber Assets simply because they do not directly perform a Reliability Operating Service.

Question 5: The VOIP question would be more on colocation on hardware. (This is in reference to Question 3 above)

Response: We're not sure what you mean by this. If you mean the VOIP system is on the same network as the EMS in the Control Center (*not* a recommended practice, by the way!), then its component Cyber Assets will be Protected Cyber Assets. But that still doesn't make them BES Cyber Assets. If you meant something else, please email karl@energysec.org.

Question 6: What is the latest regarding...2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above?

Response: This is still a matter of great controversy. NERC issued a memorandum last month that attempted to set the matter straight, but we don't believe it has done that. EnergySec will be considering the need for a formal interpretation request on this topic. If you're interested in participating in that effort, contact steve@energysec.org

Question 7: Is that still enforceable moving forward after the Memo? (This is a follow-on to Question 6)

Response: That's what the controversy is about. A bigger question is whether NERC can declare a particular guidance to be "enforceable" when it doesn't result directly from an RFI. See question 13 below.

Question 8: Are you planning a webinar on the impacts of the "Network and Externally Accessible" memo?

Response: That memo probably requires a book all by itself. However, we may address one or two aspects of that memo in our second webinar on June 18.

Question 9: Considering the RFI only considers what is within the 4 corners of the Standard...is there enough latitude in that process to clarify the technical concerns?

Response: We're assuming you're referring to the general discussion of how NERC can address the many interpretation questions in CIP version 5. We totally agree with you that it will be very hard for RFIs to address technical concerns, since usually they are about something more than just the strict meaning of a requirement (which is what RFIs address). Some technical issues can be dealt with through new Definitions; others may require standard revisions. Either of those will require a Standards Authorization Request (SAR).

Question 10: If a facility is impacted, say a breaker is tripped, but the transmission system can still be operated per the RC's SOL methodology, would it be appropriate to say that there is no BES Cyber Asset?

Response: We don't think so. As discussed in our response to Question 1 above, the BES Cyber Asset definition refers to "impact on a Facility, system, or equipment", not to "impact on the BES." The threshold for becoming a BES Cyber Asset is pretty low.

Question 11: I think you may have mentioned a SAR is more likely to be helpful.

Response: We no longer know the context of this question, but in general this is true. As discussed in our response to Question 9, in many cases the only good way to deal with a particular question of interpretation of CIP version 5 will be through a SAR.

Question 12: What is the list of items that are still open for interpretations? ERC? Serial in scope? Network communications in scope? Virtualization? What else still needs to be written out in a LL or FAQ?

Response: There are unfortunately probably hundreds of open interpretation items for CIP Version 5. And their number keeps increasing as NERC entities pursue their compliance programs in more depth. We would like to see NERC keep a running list of all interpretation questions that have been reported to it. Bear in mind that formal Interpretations need to be requested via the process outlined in the Rules of Procedure. EnergySec has initiated one RFI, and is considering submitting additional RFIs in collaboration with interested entities. However, given the multiyear timeframe for getting Interpretations resolved, there needs to be some process by which guidance is provided, which the NERC entities and Regions have generally agreed is legitimate and is something they will strive to follow. We had hoped the Lessons Learned – with their process for industry comments and revisions – would be the agreed-upon process. However, NERC seems to be rethinking this (see the next question).

Question 13: The NERC BOT (Board of Trustees) just created a new team to finalize these open issues. How is that supposed to work moving forward?

Response: Unfortunately, the new team isn't tasked with finalizing open issues. Rather, they are tasked with determining how NERC will provide guidance for reliability standards going forward. We don't know whether or not current guidance processes like the Lessons Learned and FAQs will be suspended pending this team's final report (due in August). However, NERC entities will need to continue working on CIP Version 5 compliance by the April 1, 2016 date as best they can, since we have not heard anything about that date being pushed back.