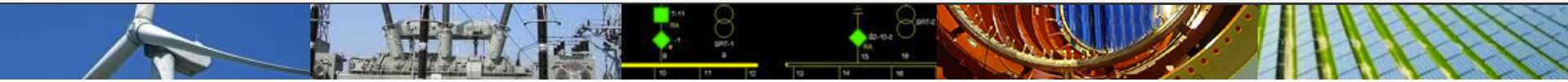
EnergySec
The National Energy Sector Cyber Security Organization

What Does the FERC CIP v6 NOPR tell us?



EnergySec Webinar
August 19, 2015

Meet Your Panelists

Tom Alrich
Manager Cyber Risk Services
Deloitte and Touche LLP

Karl Perman
VP, Services
EnergySec

Steve Parker
President
EnergySec

It's Interactive

Please submit your questions through the control panel to get answers LIVE from our panelists.

It's Hip to Chat

EnergySec is hosting an online chat to accompany this webinar which is open to all registered EnergySec Community participants.

To join the chat as a guest, visit:

https://hipchat.energysec.org/gntQ4VQHo

If you have a HipChat account already, join us in the FERC V6 NOPR room. Note: Registered users have access to the chat history, file attachments, and links.

Deloitte.

What Does the FERC CIP v6 NOPR tell us?

Tom Alrich
Manager
Cyber Risk Services
Deloitte & Touche LLP
August 19, 2015

Agenda

- Summary of the NOPR
- Why did FERC issue a NOPR, not an Order? – Tom will lead
- What does FERC have in mind for protecting "communications networks" between Control Centers? – Steve and Karl will lead
- Why is FERC concerned about NERC's definition of LERC? What might it mean for ERC? – Tom will lead
- Why are there so many acronyms that end in ERC?

Before I Begin – a Shameless Plug

- I will be leading a three-hour workshop the afternoon of September 14, the first day of EnergySec's Security and Compliance Summit in Washington, DC.
- I'll be joined by Matt Light of Deloitte – formerly with NERC and before that DoE.
- We'll be discussing "implicit requirements" in CIP versions 5 and 6 – that is, things an entity needs to do to comply with the written requirements, but which themselves aren't written down. As you might guess, there are *lots* of these.
- Matt and I will provide our opinions on how to address these – but we'll also want to hear from you on implicit requirements you've discovered, and how you're addressing them.
- There's a $300 fee for this, but it all goes to EnergySec – a good cause!

What's in the NOPR?

First, FERC intends to approve the seven CIP v6 standards.

Second, they ask for comments on a requirement to protect "communications networks" between Control Centers.

Third, they request comments on a possible need to strengthen the protections required for Interactive Remote Access.

Fourth, they ask for comments on a possible new standard to address security of the supply chain.

Fifth, they ask NERC to clarify what the word "direct" means in the definition of Low impact External Routable Connectivity (LERC).

Sixth, they request comments on extending Transient Device controls to Low impact BES Cyber Systems.

This webinar addresses 1,2, and 5. We hope to address 3, 4 and 6 in a future webinar.

Why Did FERC Issue a NOPR, not an Order?

- A NOPR is…An Order is….
- Many in the industry expected FERC to issue an Order approving CIP v6, not a NOPR saying they *intend* to approve it.
- FERC did ask for comments on several possible changes to v6. So it is possible they want to first decide on these changes before they approve it (but the changes would appear in a new v7, not in v6. And FERC could have ordered them while still approving v6).
- They also brought up an entirely new topic, supply chain security. A NOPR is definitely appropriate for this, but why did they piggyback it on the v6 NOPR? Why not issue a separate one?
- The biggest mystery is due to the fact that, if v6 isn't approved in Q4 (probably October), the main compliance dates for v6 will be moved back. Since comments on the NOPR aren't due until late September, this leaves almost no time for FERC to digest the comments and make their decisions.

What if FERC Wants to Move the v5/6 Date Back?

WARNING: This slide amounts to rank speculation. However, it is interesting to consider…

- It is strange that FERC would ask for comments on some heavy issues, then leave themselves almost no time to consider them – *if* they want to leave the v6 compliance dates unchanged.
- This isn't so strange if FERC actually plans to spend the normal amount of time considering comments (6-9 months) – meaning they would approve v6 around mid-2016.
- But this would mean the v6 compliance dates would be moved back. If FERC approved v6 next summer, the v6 date would be 1/1/17 or even 4/1/17.
- However, the v5 standards will still come into effect 4/1/16. This means there would be a 6-12 month gap between the v5 and v6 dates. How can this work?

What if FERC Wants to Move the v5/6 Date Back?

- I have advocated for a while that the compliance date for CIP v5 needs to be moved back from April 1, 2016. I say this because there are many fundamental issues regarding the interpretation of the CIP v5 standards (especially CIP-002 R1 and CIP-005 R1) that haven't been properly addressed by NERC.
- I have suggested that one way to do this would be to follow the model from the CIP v1 rollout: have a Compliant date, followed by an Enforceable date a year later. The Compliant date would remain 4/1/16, but the Enforceable date would be later.
- For this to happen, it would require explicit action on NERC's and FERC's part – I'll admit this is a long shot.
- But I've also said I expect *the enforcement date will still effectively be moved back* regardless of NERC's and FERC's actions – since the regions won't have the appetite to aggressively enforce violations caused simply by confusion about the requirements.

What if FERC Wants to Move the v5/6 Date Back?

- But If FERC effectively pushes the v6 date back 6-12 months by delaying approval of v6, I think NERC – or maybe some of the regions – may explicitly state they are delaying enforcement of v5 to avoid the situation where entities have to comply with v5 standards, then v6 not too long after that.
- Bottom line: Whether or not FERC delays approving CIP v6 beyond Q4, and whether or not NERC makes any explicit statement about delaying enforcement of v5, I believe the enforceable dates for CIPs v5 and v6 will effectively be moved back 6-12 months, for entities that make a *good faith* effort to come into compliance on April 1, 2016.
- If an entity clearly hasn't even tried to comply, that's a different story altogether. I'm not saying that entities can slack off their compliance efforts – it is still vitally important that you make every effort to be compliant next April 1.

What if FERC Wants to Move the v5/6 Date Back?

- The corollary to this is that NERC needs to make a big effort to provide a complete set of guidance on the v5/v6 requirements and definitions ASAP – but by 4/1/16 at the latest.
- Entities need 6 months to a year (preferably a year) of certainty, in order for compliance to be enforceable. Currently, there is huge uncertainty over many fundamental issues – the meaning of "programmable", what "affect the BES" means in the BCA definition, the meaning of ERC, etc. This needs to be cleared up before entities can truly finish their compliance programs.
- If NERC can't come out with comprehensive guidance by 4/1/16, I'll probably be back with another webinar, calling for the enforcement date to be moved back further. I'll be following NERC's progress in my blog. Maybe I'll have a thermometer showing how far they've come and how far they have to go.

“Communications Networks”

- When FERC approved CIP v5 in Order 791, they ordered NERC to require protection for “non-programmable components of communications networks”.
- NERC interpreted this narrowly to mean wiring that links devices within an ESP, but which exits the PSP. This wiring (and associated hubs, etc) isn’t physically protected under v5. In v6, NERC developed a requirement part (CIP-006-6 R1.10) requiring either physical or logical (encryption) protection of such wiring.
- FERC points out in the NOPR that networks that link ESPs aren’t protected by this requirement. They ask for comments on whether there should be a requirement to protect these networks.
- Specifically, they want comments on whether there should be a requirement to protect communications networks between Control Centers. They’re obviously considering ordering a new requirement for just that.

“Communications Networks”

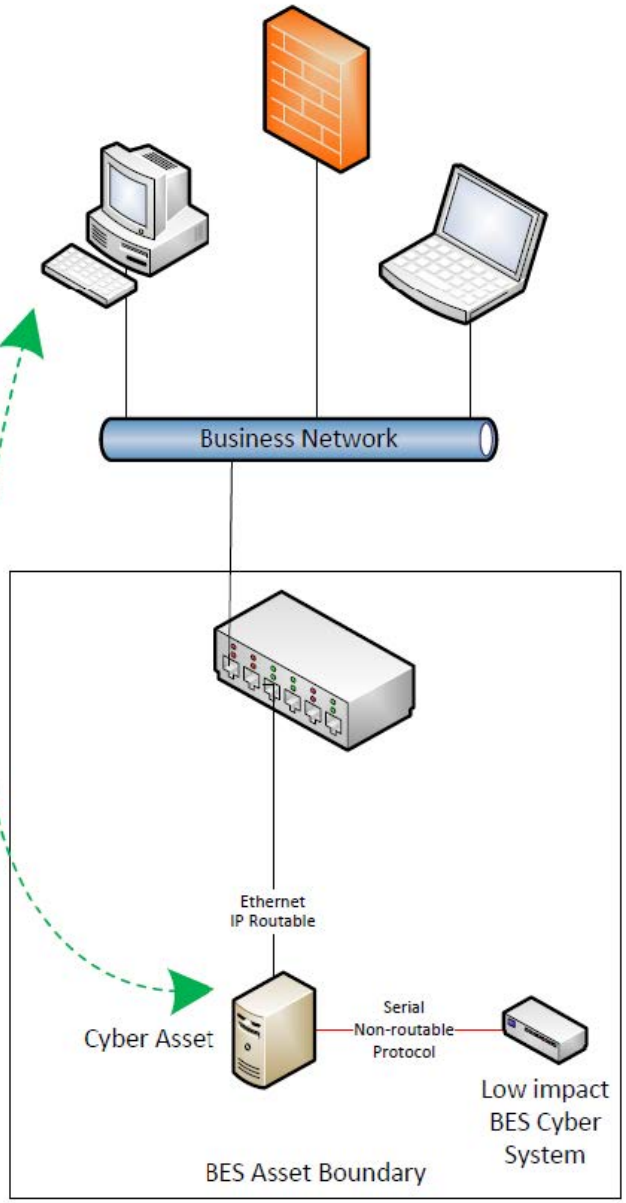
- However, FERC concedes two points up front:
- First, they admit (paragraph 57) that entities often don’t control the wiring and switching hardware that links ESPs. This means it is unlikely that physical protections can be required.
- They go on to state (paragraph 58) that logical controls can be required instead. This usually means encryption, but FERC concedes that this might cause unacceptable latency issues - given that Control Centers are involved.
- What other logical controls are there?
  - Advanced encryption
  - Active monitoring of the network
  - We would be interested in hearing more

Why doesn't FERC like LERC?

- LERC is intended to be the "equivalent" of External Routable Connectivity (ERC) for Lows. That is, it is required if a higher level of controls is going to apply. Specifically, the requirement for Electronic Access Control for Low assets in CIP-003-6 R2 (Attachment 1) only applies to those with LERC.
- FERC quotes the definition of LERC: "Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bidirectional routable protocol connection."
- FERC's issue comes down to this: What is meant by "direct"?

Why doesn't FERC like LERC?

- FERC points to Reference Model 6 *(we'll show it on the next slide)* on page 36 of CIP-003-6, where NERC states "In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example."
- FERC states (paragraph 70) that this "may conflict with the plain reading of the term 'direct.'" Specifically, they ask for comments on the meaning of "layer 7 application break", and why NERC believes that this "breaks" the "direct" connection. If NERC can't convince FERC that the direct connection is in fact broken in this "application break", it seems likely FERC will order that a new definition of LERC be drafted, including an interpretation of "direct" that is acceptable.



Data Flows

REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.

Why doesn't FERC like LERC?

Tom's Opinion:

- NERC has all along wanted to avoid any wording that would lead to an inventory of Low impact BES Cyber Systems being required. This is why the Low requirements apply only at the asset level, not the cyber asset level.
- However, if NERC wants to distinguish between assets with ERC and those without it using concepts like protocol break, they will *inherently* be requiring a BCS inventory, since this concept only applies on the cyber asset level. And an ESP may also be required.
- IMHO, it is best for NERC to simply state that, whenever there is ERC coming into a Low asset, there is LERC – period. I don't believe there is any possible "definition" of "protocol break" that NERC can provide, that will not immediately lead to the requirement for an inventory of Low BES Cyber Systems.

What might this mean for ERC?

Tom's Opinion:

- "External Routable Connectivity" is a NERC defined phrase, although many entities have not found it to provide sufficient guidance – especially in the case where a relay in a substation is connected serially to a device like an RTU or protocol converter, which then is routably connected to a Control Center.
- In our last webinar, we discussed the concept of "protocol break", and agreed that was useful in distinguishing cases with ERC from those without ERC.
- It seems obvious that FERC doesn't agree with this idea. In theory, FERC doesn't have any say on ERC at this point, but… Since the meaning of ERC still needs to be clarified by NERC, they may want to look seriously (again) at FERC's wording in the NOPR. This means they may come back to something like the discussion of ERC in the Memorandum from April.

Conclusions

- The fact that FERC didn't approve CIP v6 in July, but instead issued a NOPR saying they were going to do that, combined with the fact that they have left themselves very little time to digest the comments they will receive, raises the question whether FERC will not approve CIP v6 until next year – leading to the v6 implementation date being pushed back. In any case, we believe the *effective* enforcement date for v5 and v6 will be later than 4/1/16 – but compliance is still required on that date.
- FERC is clearly considering ordering a requirement to protect "communications networks" between Control Centers, but it is unclear by what means this goal could be accomplished.
- FERC doesn't like the idea that a "protocol break" would result in no LERC being present, and has asked for comments on this. But it isn't clear NERC can provide *any* definition of protocol break which won't result in the need to inventory Low BCS and possibly have ESPs at Low assets.

Questions

Contact Us

Sharon Chand
Director
Deloitte & Touche LLP
+312 486 4878
shchand@deloitte.com

Eric Bowman
Senior Manager
Deloitte & Touche LLP
+1 206 716 7839
ebowman@deloitte.com

Tom Alrich
Manager
Deloitte & Touche LLP
+1 312 515 8996
talrich@deloitte.com

Deloitte.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Thank You

Tom Alrich
talrich@deloitte.com
312.515.8996
www.deloitte.com

Karl Perman **Steve Parker**
503.905.2000
www.energysec.org