ENERGYSEC
THE NATIONAL ENERGY SECTOR CYBER SECURITY ORGANIZATION

CIP V5
The Top Issues with CIP-003 – CIP-011 and What You Can Do About Them

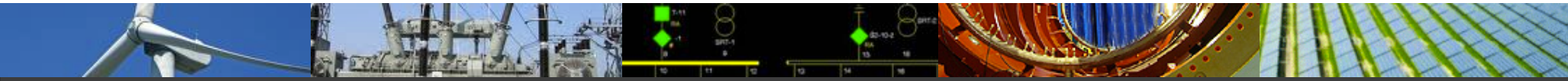
EnergySec Webinar
June 18, 2015

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.

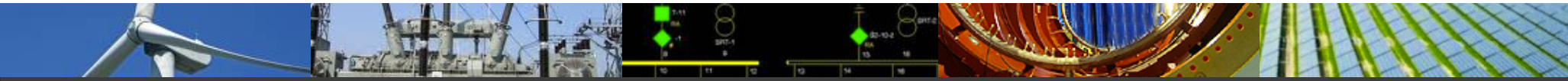
It's Hip to Chat

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/gS8XuuofH

If you have a HipChat account already, join us in the ES Webinar 6-18-15 room. Note: Registered users have access to the chat history, file attachments, and links



Deloitte.

Some top issues with CIP-003-6 through CIP-011-2

and what you can do about them

Tom Alrich
Manager
Cyber Risk Services
Deloitte & Touche LLP
June 18, 2015

Agenda

- Introduction
- NERC's "Network Devices" Memorandum – four questions
- NERC's answers to the four questions
- Conclusions

Copyright © 2015 Deloitte Development LLC. All rights reserved.

Introduction

- In our May webinar, someone asked if we would address the NERC Memorandum on “Network Devices” in this webinar.
- I’ve recently made the rounds of the WECC and SPP meetings on CIP version 5, as well as the NERC CIPC.
  - The April Memoranda were by far the biggest current concern of the entities there.
- The two Memoranda causing the most heartburn are the ones on “Programmable Electronic Devices” – which we discussed in the May webinar – and on Networking Devices.
  - We will focus on the Network Devices Memorandum in this webinar.

Copyright © 2015 Deloitte Development LLC. All rights reserved.

Memorandum Number 4: “Network and Externally Accessible Devices”

This Memorandum purports to address three questions, but it is actually four:

- Q1: Can networking devices be BES Cyber Assets?
- Q2&3: Two questions about Section 4.2.3.2, which exempts network devices between ESPs from the standard.
- Q4: If a natively serial-based BCA has been “modified” (with a device like a protocol converter) to be externally accessible via a routable network, can it be said to have External Routable Connectivity?

Copyright © 2015 Deloitte Development LLC. All rights reserved.

Q1: Can Networking Devices be BES Cyber Assets?

- NERC says yes, and I agree with this.
- I don't agree with how they came to that conclusion.
  - Their understanding of how you determine whether there can be "adverse impact" is very different from mine.
- I discussed this topic at length in the previous webinar, so I won't repeat that argument now.
  - You can listen to the recording here: http://grids.ec/cip002_recording

Copyright © 2015 Deloitte Development LLC. All rights reserved.

Q2&3: Regarding Section 4.2.3.2

- Section 4.2.3.2 (of each CIP v5 standard) reads “Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (are exempt from each of the CIP v5 standards).”
- The first question NERC answers is “If a device subject to the exemption would otherwise be a BCA and have to be in an ESP, does the exemption “override” the BCA designation?
- NERC’s answer to that is no, and I agree.
  - We’re talking about devices within or on the edge of an ESP.
  - These obviously aren’t between ESPs, so they can’t be exempt from VIP version 5.

Copyright © 2015 Deloitte Development LLC. All rights reserved.

Q2&3: Regarding Section 4.2.3.2

- The second question on 4.2.3.2 is harder: “Does the exemption apply to cyber devices associated with non-routable communications links?”
- I interpret this to mean, “If a network device isn’t between two ESPs because there are no ESPs, but it nevertheless links two assets – like a control center and a substation - is the exemption denied to it?
- Based on the strict wording of the exemption, the answer would seem to be “yes”.
  - But NERC makes the argument that there is a “parallel exemption” for non-routable communications devices; they will therefore use their “discretion” to exempt such devices.
- As with the first question, I agree with NERC’s answer, but I don’t agree with their reasoning that got them there.

Copyright © 2015 Deloitte Development LLC. All rights reserved.

Q2&3: Regarding Section 4.2.3.2

- NERC states on p. 5: the network devices in question are typically “owned and controlled by third-party providers (common carrier).”
  - While they don’t directly say it, they seem to be pointing to paragraph 4.2, which states that only “Facilities, systems and equipment owned” by a Responsible entity are in scope for v5.
- The problem with this is that there are a lot of wide-area communications devices that *are* owned by NERC entities.
  - Do these have to be treated as BCS, have their own ESP, etc?
- Fortunately, there is a better argument. CIP-002 R1 lists six types of assets. BES Cyber Systems that aren’t located at one of these six asset types aren’t in scope for v5.
  - Since the network devices in question are never located at one of the six assets, they’ll be out of scope.
  - But note what the Memorandum says about “demarc points”.

Copyright © 2015 Deloitte Development LLC. All rights reserved.

Q4: “Natively serial-based BCAs”

- The fourth question NERC addresses in the Memorandum regards serially-connected devices (e.g. in a substation) that are externally accessible by electronic means - in what cases can they be said to have External Routable Connectivity (ERC)?
- ERC is defined as “The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated ESP via a bi-directional routable protocol.”
- I will discuss my take on this question, then turn it over to Steve and Karl.

Copyright © 2015 Deloitte Development LLC. All rights reserved.

Q4: “Natively serial-based BCAs”

- NERC focuses on devices that just translate routable communications to serial, saying that a serial-only device has thereby been transformed into one that is routably accessible. I don’t argue with this position.
- However, Morgan King of WECC gave a good presentation in January that distinguished between devices that merely translate protocols, and ones that actually “break” the routable protocol and initiate serial communications with the relay (such as, in some cases, an RTU or a communications processor).
  - With the former devices, there’s ERC. With the latter, there isn’t.
  - You do have to look at what the device actually does, to determine whether or not it “breaks” the routable protocol.

Copyright © 2015 Deloitte Development LLC. All rights reserved.

Conclusions

- NERC's Memorandum on "Network and Externally Accessible Devices" provides answers to four questions.
- For the first three questions, I agree with NERC's answers, but not with NERC's reasoning in arriving at those answers.
- For the last question – regarding ERC – I agree with NERC's answer, but I think you need to go beyond the one example they gave – and that leads to a different answer.

Copyright © 2015 Deloitte Development LLC. All rights reserved.

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

Copyright © 2015 Deloitte Development LLC. All rights reserved.

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.

Copyright © 2015 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited

Questions

Thank You

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

Karl Perman
karl@energysec.org
503.905.2000
www.energysec.org