The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Low Impact Update

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resiliency, and sustainability of your CIP compliance programs. There are times that I may also discuss areas of the standards that other entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes stormy waters of CIP compliance.

On April 19, 2018, FERC issued Order 843 approving CIP-003-7, Security Management Controls. See the article on pages 11 and 12 of this Newsletter for details. In recognition of this action, I'll explore multiple questions related to low impact BES Cyber Systems.

Physical and Electronic Access Controls Implementation Date

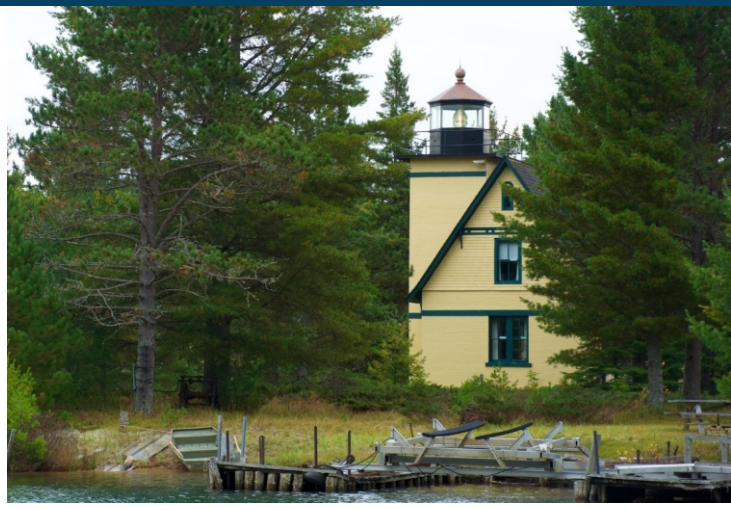
Q With FERC approving CIP-003-7, do I still need to put physical and electronic access controls in place for my low impact BES Cyber Systems by September 1st of this year?

A No. Neither the physical access controls of CIP-003-6 Attachment 1 Section 2 nor the electronic access controls of CIP-003-6 Attachment 1 Section 3 will go into effect. Instead, these controls have been replaced by CIP-003-7 Attachment 1 Sections 2 and 3, with an effective date of January 1, 2020. You have an extra 16 months to put these controls in place. However, I recommend that you do not interrupt or postpone your efforts to bring your assets with low impact BES Cyber Systems into compliance. Instead, use this gift of time to put your controls in place and test them thoroughly. You can test different approaches and see what works (and what doesn't) without a compliance risk. You can also use this time to mature these controls so that they are an integral part of your operations, similar to a pre-job safety briefing.

FERC-ordered Study of Electronic Access Controls

Q Why did FERC order a study to assess the implementation of CIP-003-7?

A Without asking the Commission directly, we can't know for sure. But we can make some inferences based on the public documents available.



Mandan, MI - Photo: L. Folkerth

In its Notice of Proposed Rulemaking (NOPR) for CIP-003-7, FERC expressed concern that CIP-003-7 Attachment 1 Section 3.1 "does not appear to contain clear criteria or objective measures to determine whether the electronic access control strategy chosen by the [R]esponsible [E]ntity would be effective for a given low impact BES Cyber System to permit only necessary inbound and outbound connections" (NOPR, P. 29). In particular, I believe FERC was concerned about the phrase "as determined by the Responsible Entity" (NOPR, P. 24-26) and about a lack of objective measures to assess compliance (NOPR, P. 28-29).

Instead of ordering more stringent language in Section 3, FERC was persuaded to let industry implement the existing language (Order 843, P. 27-30). FERC also established several very clear expectations:

- Responsible Entities are expected to be able to provide a technically sound explanation as to how the electronic access controls meet the security objective.
- NERC and the Regional Entities will have the ability to assess the effectiveness of the electronic access control plan required by CIP-003-7 R2.
- NERC and the Regional Entities will have the ability to assess an entity's adherence to its electronic access control plan.

In order to verify that these expectations are being met, NERC is required to perform the study you asked about. The study will include:

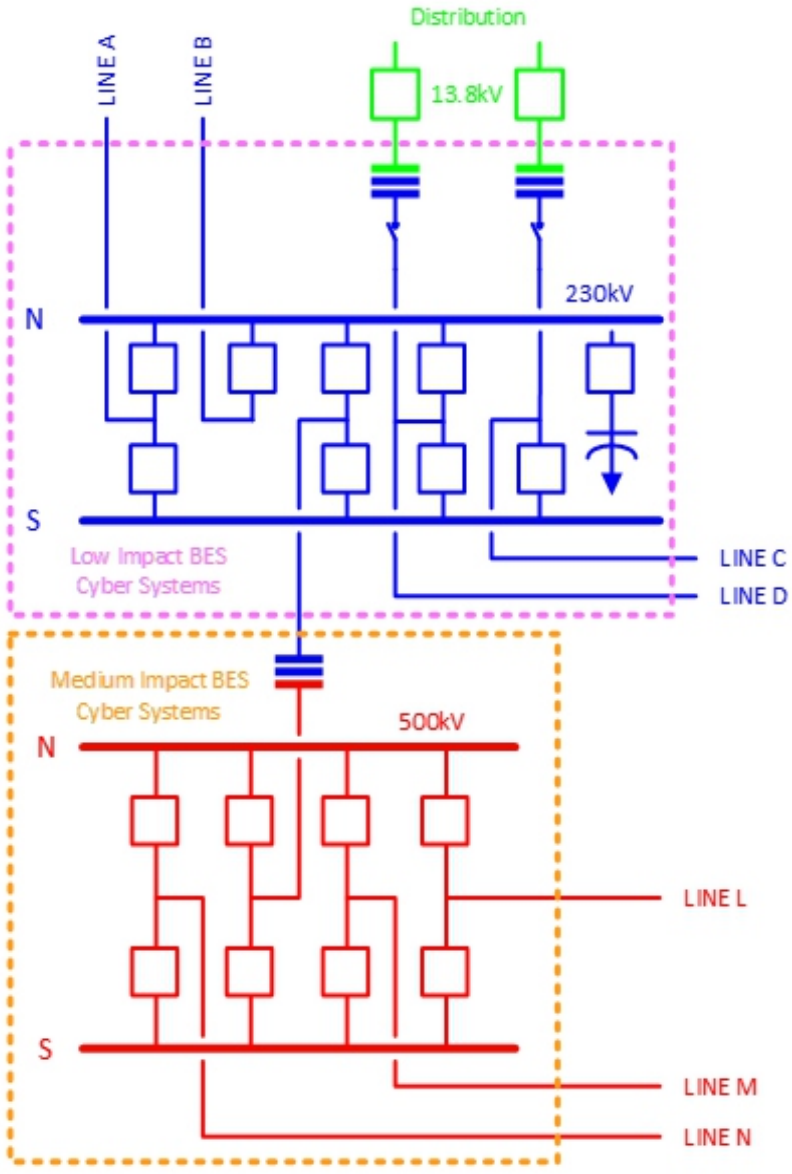
- What electronic access controls entities choose to implement;
- Under what circumstances these controls are implemented;
- The adequacy of these controls; and
- Other relevant information.

When audits of your electronic access controls for low impact BES Cyber Systems

Continued on page 15

Continued from page 14

Figure 1



begin in 2020, you should expect them to be very detailed and thorough. The audit teams will not only be reviewing your compliance with the Standard and its associated controls, they will be gathering information to provide to NERC for its study.

Impact of IRC 2.4 on Low Impact BES Cyber Systems

Q Does the presence of 500kV or above bring an entire substation up to medium impact?

A No, not by itself. According to CIP-002-5.1a Attachment 1 Impact Rating Criterion (IRC) 2.4, BES Cyber Systems associated with substation Facilities operating at 500kV or more will be assigned a medium impact rating. Note the capital "F" of Facilities calls out the Glossary definition, "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)" These Facilities will include any transformer with a high side at 500kV or more, and breakers, reactors, capacitors, etc. operating at 500kV or more.

However, BES Cyber Systems associated with the remaining Facilities within the substation will be evaluated according to IRC 2.5. IRC 2.5 contains two criteria. In order to meet IRC 2.5, a substation must connect at 200kV or higher to three other substations. If this is true, then an aggregate weighted value is calculated based on the number of lines crossing the substation boundary and the voltage level of those lines. If this aggregate weighted value exceeds 3000, then the BES Cyber Systems associated with Facilities at that substation receive a medium impact rating. Otherwise, those BES Cyber Systems receive a low impact rating per IRC 3.2.

For example, the substation in Figure 1 connects to seven other substations by 230kV and 500kV lines. Each line is protected by breakers. There is a capacitor on the 230kV side of the transformer. BES Cyber Systems associated with the 230kV/500kV transformer and the 500kV breakers will have a medium impact rating. Since the substation is connected to three or more other substations at voltages above 200kV, we need to calculate the aggregate weighted value of the substation. We do The aggregate weighted value for this substation does not exceed 3000. Therefore the BES Cyber

Line	Line Voltage	Line Weight Value
A	230kV	700
B	230kV	700
C	230kV	700
D	230kV	700
L	500kV	0
M	500kV	0
N	500kV	0
Distribution	13.8kV	Out of Scope
Aggregate Weighted Value		2800

Systems associated with the 230kV breakers and the 230kV capacitor will be assigned a low impact rating.

List of Low Impact BES Cyber Systems

Q Is a list of low impact BES Cyber Systems required?

A Based on the notes attached to CIP-002-5.1a R1 and CIP-003-7 R2, the audit teams cannot require a list of low impact BES Cyber Systems at an asset. If we take a close look at CIP-003-7 Attachment 1 Section 3, however, we see

Continued on page 16

Continued from page 15

that electronic access controls are required for any routable communications that are between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber Systems. If you take the approach that any routable communications crossing the asset boundary may originate or terminate at a low impact BES Cyber System, and control electronic access accordingly, then you will not need to identify individual BES Cyber Systems, but only the assets containing low impact BES Cyber Systems.

At a generator or substation, you have the flexibility within the language of the Standard to say that not all communications are to low impact BES Cyber Systems. In order to take advantage of this flexibility you need to know which Cyber Assets are members of low impact BES Cyber Systems so that you can control electronic access to those Cyber Assets. You must be able to provide sufficient, appropriate evidence that you are protecting communications to low impact BES Cyber Systems. In order to provide this evidence you will need to know, and provide evidence regarding, which Cyber Assets are part of a low impact BES Cyber System and which are not.

One way of thinking of this is to differentiate whether you provide low impact protections at the asset (substation or generator) level or at the BES Cyber System level. If protections are at the BES Cyber System level, then you will need to be able to identify the Cyber Assets being protected. There are several places within CIP-003-7 Attachment 1 that permit compliance at the BES Cyber System level:

- Section 2, Physical security controls, permits an entity to control access to the locations of the low impact BES Cyber Systems at the asset;
- Section 3, Electronic access controls, permits an entity to control electronic access to a low impact BES Cyber System; and
- Section 5, Transient Cyber Asset and Removable Media malicious code risk mitigation, requires mitigation of the threat of the introduction of malicious code to low impact BES Cyber Systems.

In each of these cases, if you treat all Cyber Assets at an asset as low impact BES Cyber Systems, then you will not need to identify individual BES Cyber Systems to your audit team. However, if the Cyber Assets at an asset are treated differently based on whether they are members of a low impact BES Cyber System, then you will need to be able to identify those systems are that are required to be protected.

Initial Test of Incident Response Plan

Q Does the approval of CIP-003-7 alter the required date for the first test of my Cyber Security Incident response plan for low impact BES Cyber Systems?

A No, the first test of your incident response plan was due on April 1, 2017. This is not changed by CIP-003-7.

The CIP-003-5 Implementation Plan (available here) on page 2 states that the initial performance of periodic requirements in CIP-003-5 R2 is the effective date of CIP-003-5 R2, which was April 1, 2017. The CIP-003-6 Implementation Plan (available here), on page 10, incorporates the CIP-003-5 Implementation Plan by reference.

The CIP-003-7 Implementation Plan (available here) states, "The effective dates or phased-in compliance dates within the CIP-003-6 Implementation Plan, remain in effect except that the compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7."

This makes it clear that the compliance dates for Section 4 do not change with CIP-003-7's approval.

If you did not understand this and have yet tested your low impact Cyber Security incident response plan, I strongly recommend that you perform a test as soon as practical. You should also contact the RF Enforcement Group to discuss and work through any potential noncompliance.

I also recommend testing your plan much more frequently than the Standard requires. It is important for even low impact BES Cyber Systems to have a usable and effective Cyber Security Incident response plan, and to have a trained and proficient incident response team to carry out the plan.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated.

I may be reached here.